VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2020 Bc. Marek Vitula

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV RADIOELEKTRONIKY
DEPARTMENT OF RADIOENGINEERING

CHYTRÝ ZÁMEK VYUŽÍVAJÍCÍ SÍTĚ IOT
SMART DIGITAL DOOR LOCK SYSTEM USING IOT NETWORKS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Marek Vitula**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Filip Záplata, Ph.D.**
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Elektronika a sdělovací technika**

Ústav radioelektroniky

Student: Bc. Marek Vitula ***ID:*** 186596
Ročník: 2 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Chytrý zámek využívající sítě IoT

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s nabídkou nízkopříkonových mikrokontrolérů, NFC čteček a transceiverů pro IoT síť Sigfox od firmy NXP. Prostudujte možnosti stávajících elektromechanických zámků a zvolte vhodný zámek, který bude možné elektronicky ovládat. Navrhněte řešení elektronického zámku, který bude umožňovat autorizaci pomocí NFC tagu a následné otevření zámku a odeslání informace o provedení úspěšné či neúspěšné autorizace do sítě Sigfox. Zohledněte možnosti bateriového napájení zařízení a také možnosti zařízení vestavět do dveří.

Realizujte elektroniku pro vybraný zámek a implementujte firmware v jazyce C. Vyberte vhodné antény pro NFC a Sigfox IoT na základě požadavku vestavby do dveří. Otestujte čtení NFC tagu a komunikaci se sítí Sigfox. Diskutujte bezpečnost navrženého řešení.

DOPORUČENÁ LITERATURA:

[1] KHAN, Gul N. a Krzysztof INIEWSKI, ed. Embedded and networking systems: design, software, and implementation. Boca Raton: CRC Press, c2014. ISBN 978-1-4665-9065-6.

[2] ZÁHLAVA, Vít. Návrh a konstrukce desek plošných spojů: principy a pravidla praktického návrhu. Praha: BEN - technická literatura, 2010. ISBN 978-80-7300-266-4.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 14.5.2020

Vedoucí práce: Ing. Filip Záplata, Ph.D.

prof. Ing. Tomáš Kratochvíl, Ph.D.
předseda oborové rady

ABSTRAKT

Tato diplomová práce se zabývá návrhem bateriově napájeného chytrého zámku využívajícího sítě IoT a technologii NFC pro autentizaci uživatele. V první části popisuje jednotlivé komponenty, které budou použity pro návrh zařízení a dále se zabývá návrhem přizpůsobovacích obvodů a antény pro NFC. Další část práce se věnuje návrhu zapojení a následně návrhu desky plošných spojů. Třetí část práce popisuje firmware a závěrečná část je věnována rozboru bezpečnosti.

KLÍČOVÁ SLOVA

Chytrý zámek, chytrá domácnost, IoT, Internet věcí, Sigfox, NFC, Kinetis, NXP, Mifare

ABSTRACT

This master thesis describes the design of a battery-powered smart lock using IoT networks and NFC technology for user authentication. The first part of the thesis describes the individual components to be used for the device design and also deals with the design of matching circuits and the antenna for the NFC. The following part of the thesis describes the design of the hardware, particularly the design of the printed circuit board. The third part describes the firmware and the final part of the thesis is dedicated to the security analysis.

KEYWORDS

Smart lock, smart home, IoT, Internet of Things, Sigfox, NFC, Kinetis, NXP, Mifare

VITULA, Marek. *Chytrý zámek využívající sítě IoT*. Brno, Rok, 95 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky. Vedoucí práce: Ing. Filip Záplata, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Chytrý zámek využívající sítě IoT“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce panu Ing. Filipovi Záplatovi, Ph.D. a konzultantům Ing. Viktorovi Obrovi a Ing. Janu Nevoralovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

podpis autora

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Po krátkém úvodu a seznámení se zadáním práce následuje první kapitola, která se věnuje výběru vhodných hardwarových komponent s důrazem na bateriové napájení celého zařízení. Je zde také teoreticky rozebrána technologie Sigfox a NFC a rovněž je zde teoreticky rozebrán návrh antény a přizpůsobovacího obvodu pro NFC. Další kapitola se věnuje návrhu zapojení jednotlivých komponent a návrhu desky plošných spojů. V kapitole č. 3 je popsán firmware. Poslední kapitola diskutuje bezpečnost použitých technologií.

Úvod do problematiky

Diplomová práce se věnuje návrhu chytrého zámku využívající sítí IoT. Zařízením zvané jako internet věcí (Internet of Things) se přikládá stále větší význam. Dle analytické agentury Gartner bude v následujících letech trh s těmito zařízeními růst. V roce 2020 by mělo být na světě 5,8 miliard těchto připojených zařízení. Předpokládá se, že největší růst zaznamená odvětví automatizace budov. [1] Stále více se také hovoří o konceptu tzv. inteligentní domácnosti (smart home) a chytrých městech (smart cities).

Tato práce si rovněž klade za cíl ukázat aplikovatelnost technologie IoT do oblasti chytrých zámků. Sítí pro IoT se nejčastěji myslí sítě typu LPWAN (Low-power wide area networks) kam se řadí například sítě Sigfox a LoRa. V rámci práce byla vybrána sít Sigfox a to zejména z důvodu dobrého pokrytí a dobré dostupnosti komunikačních modulů.

Výstupem této práce je prototyp chytrého zámku, který bude možný použít pro zabezpečení objektu. Chytrý zámek využívá sítě Sigfox a rovněž technologii NFC pro autorizaci uživatele. Jsou využity především komponenty od firmy NXP Semiconductors.

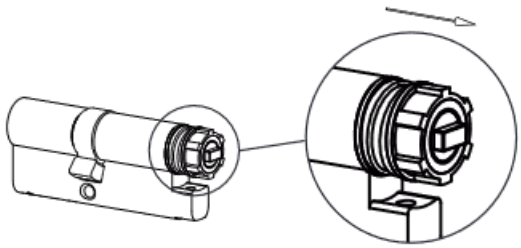
1 Teoretická část

1.1 Chytrý zámek

Chytrý zámek (Smart Lock) je označení používané pro zámky, které se ovládají elektronicky. Pro odemčení zámku se většinou používá NFC/RFID tag nebo mobilní zařízení s technologií Bluetooth, případně klávesnice pro zadání hesla či PINu. Chytrý zámek též umožňuje kontrolu a řízení přístupu do chráněného objektu.

Z hlediska řízení přístupu lze zámky rozdělit do tří kategorií: Základní zámky, které neobsahují logiku, skládají se pouze ze čtečky a vyžadují externí kontrolér, jenž provádí autorizaci a následné otevření dveří. Částečně inteligentní zámky, které umožňují otevřít dveře, avšak vyžadují externí kontrolér pro provedení autentizace. Inteligentní (Chytré) zámky, které provádějí veškerá rozhodnutí o přístupu do objektu[2].

V roce 2019 bylo na trhu dostupných několik elektronicky ovládaných zámků, které lze zabudovat do běžných dveří vybavených speciální cylindrickou vložkou. Například zámek ENTR od firmy Yale, která se zabývá zabezpečením objektů. Tento zámek je nutné použít s cylindrickou vložkou FAB ENTR, kterou pro tento účel vyvinula firma FAB, viz obr. 1.1. Z přístupové strany tohoto zámku je vstup pro klasický klíč nahrazen mechanickým převodem, ovládaným pomocí servomotoru. Další možností chytrého zámku je například zámek DANALOCK nebo zámek NUKI[3].



Obr. 1.1: Cylindrická vložka FAB ENTR [4]

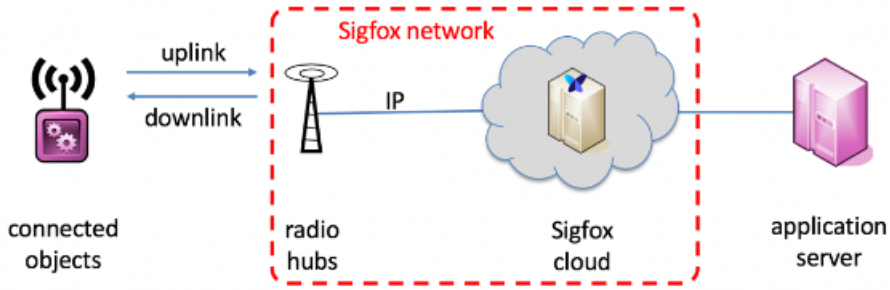
1.2 Sigfox

Tato podkapitola popisuje síť pro internet věcí – Sigfox, kterou bude navržený chytrý zámek používat pro odesílání informací o přístupu.

Sigfox je francouzská společnost, která vyvíjí bezdrátové sítě pro připojení nízkopříkonové elektroniky. Tuto elektroniku také nazýváme „internet věcí“. Mezi ně

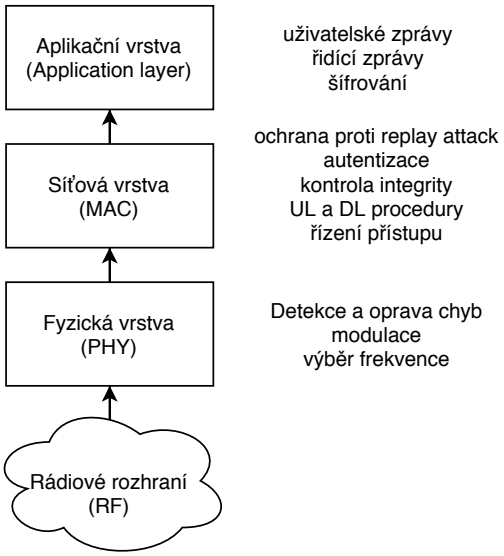
patří například elektroměry, GPS lokátory a další zařízení, které vyžadují časté odesílání malého objemu dat. V České republice je síť Sigfox provozována společností SimpleCell Networks. Síť Sigfox používá modulaci DBPSK a GFSK a používá pásmo ISM, v Evropě 868 MHz a v USA 902 MHz. Specifikace sítě Sigfox byla zveřejněna ke dnu 13. února 2019[9].

1.2.1 Specifikace sítě



Obr. 1.2: Sigfox rádiové rozhraní [9]

Na obrázku 1.2 je zobrazeno schéma sítě Sigfox. Rádiový protokol Sigfox je označen 3D-UNB. UNB značí Ultra Narrow Band, tedy velmi úzké pásmo a 3D trojitou diverzitu – časovou, frekvenční a prostorovou diverzitu. Na obrázku 1.3 jsou zobrazeny jednotlivé vrstvy sítě Sigfox – aplikační, síťová a fyzická.



Obr. 1.3: Vrstvy sítě Sigfox [9]

1.2.2 Přístup k médiu

Síť Sigfox 3D-UNB je navržena tak, aby mohla být provozována v bezlicenčních pásmech téměř po celém světě. Pro jednotlivé oblasti se místní regulace vysílání liší, firma Sigfox proto definovala tzv. rádiové konfigurace (Radio Configurations, zkráceně RC), které specifikují parametry sítě tak, aby odpovídaly místním regulacím, viz tabulky 1.1 a 1.2. Pokrytí sítě s přiřazenými rádiovými konfiguracemi je na obrázku 1.4

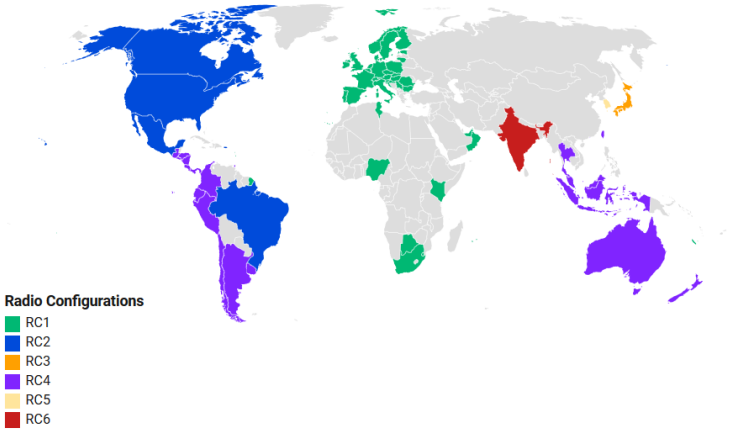
V evropských zemích je přístup k nelicencovanému spektru omezen střídou a vysílacím výkonem. Detailní popis lze nalézt v normě ETSI 300 220.

Rádiová konfigurace uplink	RC1	RC2	RC3	RC4	RC5	RC6
Start [MHz]	868,03	902,1	923,1	920,7	923,2	865,1
Střed[MHz]	868,13	902,2	923,2	920,8	923,3	865,2
Stop [MHz]	868,23	904,7	923,3	923,3	923,4	865,3

Tab. 1.1: Rádiové konfigurace pro uplink [9]

Rádiová konfigurace downlink	RC1	RC2	RC3	RC4	RC5	RC6
Start [MHz]	869,425	905,1	922,1	922,2	922,2	866,2
Střed[MHz]	869,525	905,2	922,2	922,3	922,3	866,3
Stop [MHz]	869,625	907,7	922,3	924,8	922,4	866,4

Tab. 1.2: Rádiové konfigurace pro downlink [9]



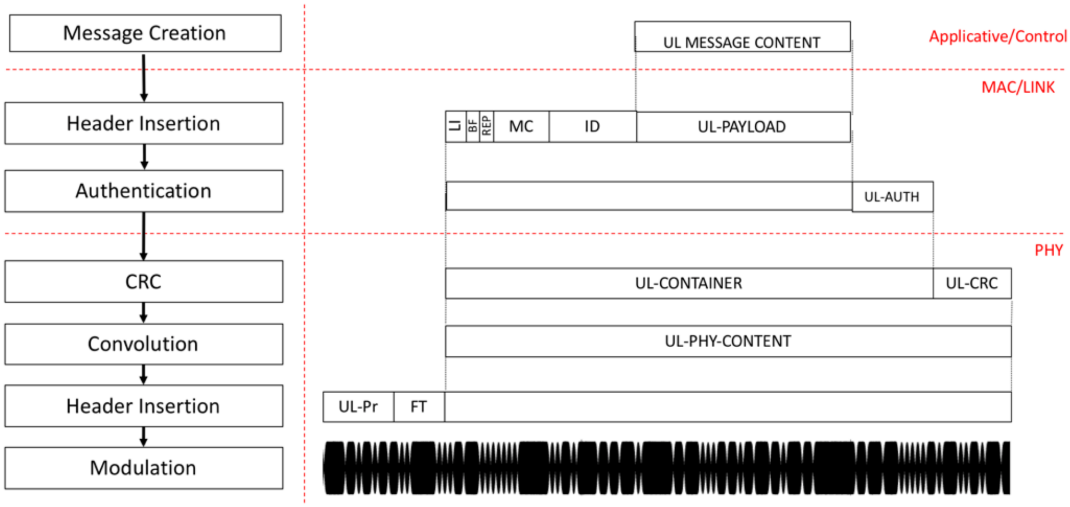
Obr. 1.4: Pokrytí sítě Sigfox [10]

1.2.3 Uplink

Modulační schéma použité v uplinku je D-BPSK s přidaným tvarováním symbolů během rotace fáze. Vysílací výkon pro RC1 je limitován na 16 dBm EIRP.

Délka uživatelsky definované zprávy (payload) v uplinku se pohybuje mezi 0 bity (prázdná zpráva) až 12 bajty. Formát zprávy je uživatelsky definovaný. Při zasílání zprávy v uplinku je možné odeslat jeden nebo tři rádiové bursty. Odeslání jednoho burstu je nejvíce energeticky efektivní, ale existuje riziko ztráty. Pro minimalizaci ztráty je možné odeslat tři bursty. Sestavení rámce v uplinku je na obrázku 1.5

Zabezpečení zpráv v uplinku je implementováno následujícími mechanismy: AES128 v módu CBC pro autentizaci a kontrolu integrity. CRC-16 pro detekci chyb při přenosu a počítadlo zpráv pro prevenci útoku přehráním.

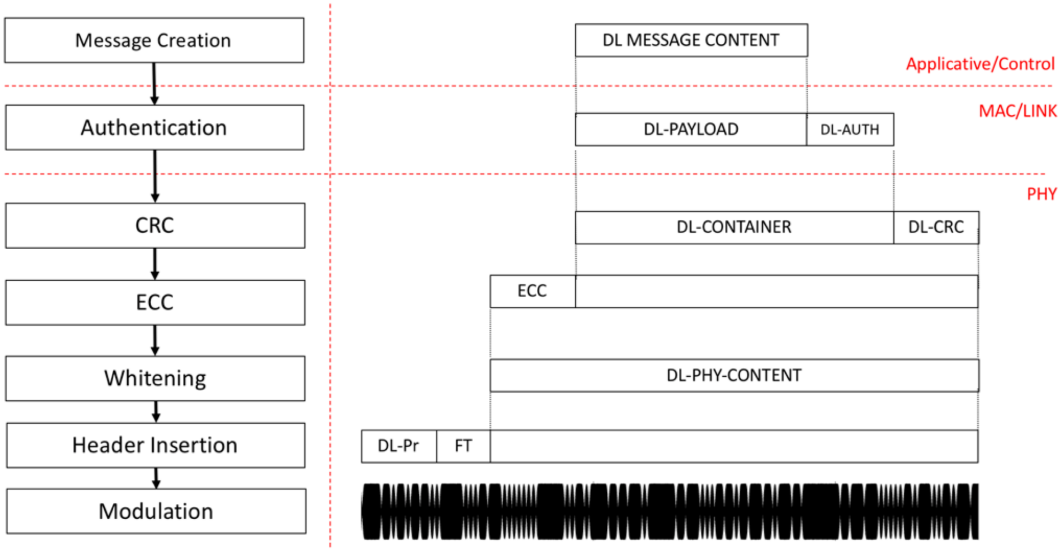


Obr. 1.5: Sigfox sestavení rámce v UL [9]

1.2.4 Downlink

V downlinku je použita modulace GFSK s odchylkou frekvence 800 Hz. Symbolová rychlost je 600 baudů.

Zpráva v downlinku má fixní délku. Sekce DL-PAYLOAD je uživatelsky definovaná. Zabezpečení zpráv v downlinku je implementováno těmito mechanismy: AES128 pro autentizaci a kontrolu integrity, BCH kódování pro opravu chyb a CRC-8 pro detekci chyb. Popis sestavení rámce v downlinku je na obrázku 1.6



Obr. 1.6: Sigfox sestavení rámce v DL [9]

1.3 NFC

NFC technologie je v chytrém zámku použita pro autentizaci uživatele pomocí tzv. tagu, neboli identifikační karty. NFC neboli Near-Field communication je technologie pro bezdrátovou komunikaci na velmi krátkou vzdálenost přibližně do 4 cm umožňující duplexní spojení mezi koncovými zařízeními a využívá se zejména pro výměnu identifikačních dat např. při finančních transakcích prováděných tzv. bezkontaktními platebními kartami nebo chytrým telefonem. Je možné využít pasivně napájené tagy, tak i tagy napájené aktivně. Komunikace probíhá na frekvenci 13,56 MHz.

NFC zařízení mohou fungovat ve třech základních režimech:

- **Emulace karty** – umožňuje zařízením podporující NFC emulovat např. platební kartu.
- **Čtení nebo zápis** – umožňuje zařízením podporující NFC zapisovat nebo číst NFC tagy.
- **Peer-to-peer** – umožňuje zařízením podporující NFC mezi sebou vytvářet ad-hoc spojení.

Komunikační protokoly používané v NFC jsou založeny na RFID standardech – ISO/EIC 14443, FeliCa, Mifare.[12]

1.3.1 NDEF

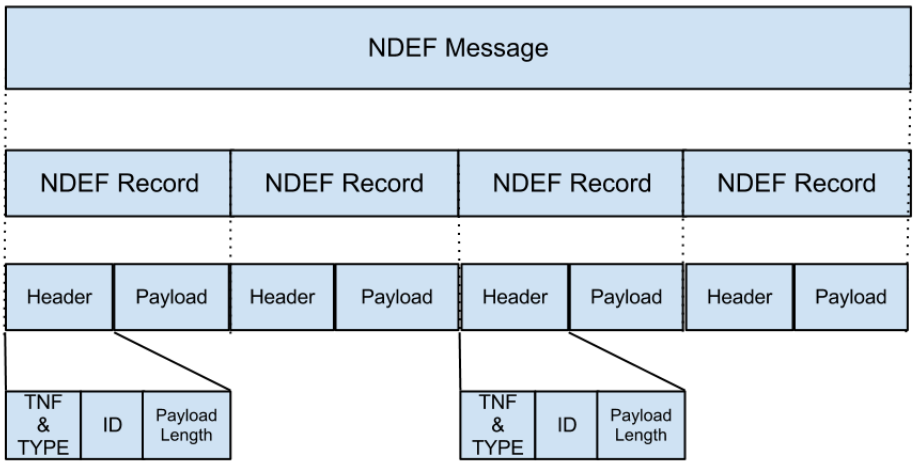
Pro výměnu informací mezi NFC zařízeními se používá formát zpráv NDEF (NFC Data Exchange Format).

Data se skládají z tzv. NDEF zpráv (NDEF Messages) a NDEF záznamů (NDEF Record) viz obr. 1.7. Každá NDEF zpráva obsahuje jeden nebo i více NDEF záznamů. NDEF záznam obsahuje tzv. payload, tedy užitečná data. Například textovou zprávu nebo URI.

Součástí NDEF záznamu je hlavička ve které jsou obsaženy informace o velikosti zapouzdřených dat (Payload length), typu dat (Payload type) a identifikátoru (Payload identification).

Typ dat je určen polem TNF (Type name format). Je standardizováno osm typů. Mezi tři nejdůležitější patří:

- EMPTY – data neobsahují žádnou informaci
- WELL KNOWN – typ podle NFC Record type definition.
- MEDIA – definováno v RFC 3986



Obr. 1.7: NDEF zprávy [36]

1.3.2 NFC tag

NFC tagy jsou pasivní zařízení které mohou být použity ke komunikaci s NFC aktivními zařízeními (čtečkami). Existují čtyři základní typy které byly definovány NFC fórem. Označují se číslicí 1 až 4 [29].

Typ 1

Tag typu 1 je založen na standardu ISO14443A. Tagy je možné číst i zapisovat. Dostupná paměť je 96 bajtů a je možné ji rozšířit až na 2 kB. Komunikační rychlost je 106 kbit/s.

Typ 2

Tag typu 1 je založen na standardu ISO14443A. Tagy je možné číst i zapisovat. Dostupná paměť je pouze 48 bajtů a je možné ji rozšířit až na 2 kB. Komunikační rychlost je 106 kbit/s.

Typ 3

Tag typu 3 je založen na systému Sony FeliCa. Dostupná paměť je 2 kB. Komunikační rychlost je 212 kbit/s. Tag typu 3 je složitější než typ 1 a 2 a tomu odpovídá i vyšší cena.

Typ 4

Tag typu 4 je ze založen na standardu ISO14443A/B. Tagy můžou být přednastaveny výrobcem tak, že na ně není možné znovu zapisovat. Dostupná paměť je 32 kilobajtů. Komunikační rychlost je mezi 106 kbit/s a 424 kbit/s.

1.3.3 MIFARE®

MIFARE je série bezkontaktních karet od společnosti NXP Semiconductors. Standard MIFARE je založen na ISO14443A. Používá šifrování AES a DES/Triple-DES a také starší standard Crypto-1, který byl prolomen v roce 2009 a není tedy považován za bezpečný.

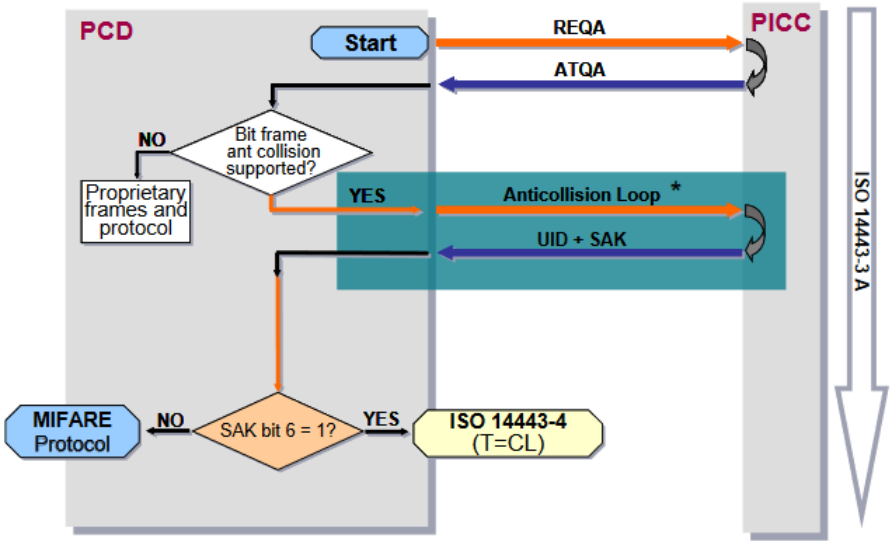
Karty MIFARE se dělí na několik variant:

- Mifare Classic – Používá proprietární protokol kompatibilní s ISO14443A. Používá šifrování Crypto-1.
- Mifare Plus – Náhrada za karty Mifare Classic se kterou je zpětně kompatibilní. Používá šifrování AES-128.
- Mifare Ultralight – Nízko nákladové karty, typicky využívané na jedno použití. Neobsahují žádné šifrování.
- Mifare DESFire – Pokročilejší systém, umožňuje šifrování AES nebo DES (varianty DESFire EV1 a EV2)

1.3.4 NFC polling

Během fáze pollingu se periodicky odesílá speciální 7bitový příkaz pro aktivaci karty REQA (request). Poté se čeká stanovený čas na odpověď. Pokud se u čtečky nachází tag, tak odpoví blokem ATQA (answer to request). Tento blok obsahuje prefix unikátního identifikátoru tagu (UID) a informaci o tom, jestli tag podporuje antikolizní protokol.

Pokud tag podporuje antikolizní protokol, tak je vyslán příkaz SELECT s prefixem UID. Pokud odpoví více tagů, tak je odesláno víc bitů z prefixu, dokud neodpoví pouze jeden tag. Tag odpoví blokem SAK (select acknowledgement). Na základě šestého bitu z odpovědi SAK je rozpoznán typ karty, pokud je hodnota bitu 1 jedná se o Mifare. V této chvíli je možné posilát další příkazy. Komunikace se ukončuje příkazem HALT. Schéma komunikace je na obrázku 1.8.



Obr. 1.8: Aktivace tagu [22]

Identifikace tagu ISO14443A

K identifikaci tagu slouží tzv. UID – unikátní identifikátor, který je přečten při antikolizi. Může být buď 4bajtový (také nazývaný NUID) nebo 7bajtový. Pro identifikaci typu tagu slouží ATQA a SAK, které jsou specifické pro jednotlivé typy tagů. Hodnoty ATQA a SAK pro systém Mifare je v tabulce 1.3.

Produkt	ATQA	SAK	ATS	délka UID
MIFARE Mini	00 04	09		4 bajty
MIFARE Classic 1k	00 04	08		4 bajty
MIFARE Classic 4k	00 02	18		4 bajty
MIFARE Ultralight	00 44	00		7 bajtů
MIFARE Plus	00 44	20		7 bajtů
MIFARE DESFire	03 44	20	75 77 81 02 80	7 bajtů
MIFARE DESFire EV1	03 44	20	75 77 81 02 80	7 bajtů

Tab. 1.3: Porovnání Mifare tagů [22]

1.4 Výběr hardware

Vzhledem k zadání diplomové práce je třeba vybrat hardware od firmy NXP. Jádrem celého zařízení je hlavní mikrokontrolér a na něj jsou kladeny tyto požadavky:

- nízká spotřeba energie v režimu spánku
- podpora periferií SPI a I2C, ideálně každou periferii dvakrát
- softwarová podpora ze strany SDK
- kompatibilita softwarového stacku Sigfox a NFC
- dostatek pinů pro obsluhu všech signálů (alespoň 15 dodatečných GPIO pinů)
- nejméně 32 kB paměti flash

Tyto požadavky nejlépe splňuje řada Kinetis Low Power nebo nová řada K32 (uvedená na trh v listopadu 2019), která je postavena na úsporné architektuře Cortex-M0+ a hodí se zejména pro bateriové aplikace. Pro tuto práci byl vybrán mikrokontrolér K32L2B, který splňuje výše uvedené body.

Firma NXP nabízí v segmentu NFC několik typů řešení:

- programovatelný mikrokontrolér s NFC, který je možný použít jako hlavní mikrokontrolér
- NFC kontrolér s integrovaným firmwarem
- NFC frontend u něhož je nutné, aby firmware NFC běžel na hlavním mikrokontroléru

Vzhledem k nedostatečné softwarové podpoře programovatelných kontrolérů s NFC, bude vhodnější zvolit řešení s integrovaným firmwarem. V nabídce NXP jsou dva mikrokontroléry s integrovaným firmwarem – PN7120 a PN7150. PN7120 je dodáván pouze v pouzdře BGA, které není příliš vhodné pro prototypovou výrobu. Alternativní PN7150 disponuje vyšším vysílacím výkonem 1,3 W ve srovnání s 0,9 W u PN7120.

Firma NXP nabízí pouze jediný nízkopříkonový RF transceiver OL2385. Možným řešením pro síť Sigfox se jeví modul SN10-11 obsahující čip NXP OL2385, jenž byl

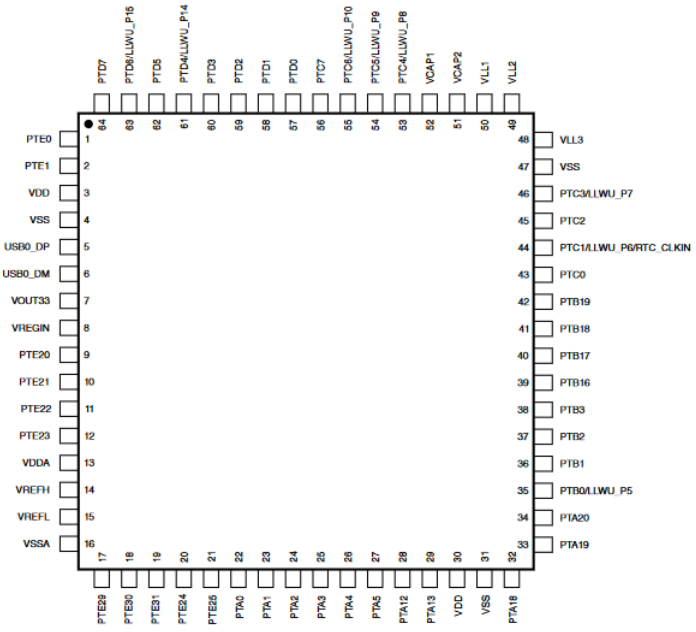
vyvíjen ve spolupráci s firmou InnoComm.

Pro řízení motorů byl vybrán dvojitý H můstek MPC17531A, jenž je kompatibilní s logickou úrovní 3,3 V. Je možné jej napájet od 2 V do 8,6 V, což vyhovuje možnosti napájení baterií. Rovněž proudový odběr v režimu spánku nepřesahující 2 µA je vyhovující.

1.4.1 Kinetis K32L2B

K32L2B je mikrokontrolér z řady Kinetis K32, vhodný pro nízkopříkonové aplikace, zejména bateriově napájenou elektroniku. Proudový odběr dosahuje pouze 1,96 µA v režimu hlubokého spánku (napájena RAM a RTC). Mikrokontrolér obsahuje úsporné jádro ARM Cortex-M0+ s taktem až 48 MHz. Řada L2B se vyznačuje podporou USB 2.0 a segmentového LCD displeje. K dispozici je několik variant, lišících se kapacitou paměti flash a SRAM 128/256 kB flash a 16/32 kB SRAM a také typem pouzdra MBGA, LQFP nebo QFN.

Mikrokontrolér obsahuje UART, dvě periferie LPUART, dva I2C moduly, dva 16-bitové moduly SPI, USB, jeden 16-bitový 16-kanálový AD převodník, vysokorychlostní komparátor a 12-bitový DA převodník a periferii FlexIO pro emulaci další volitelné periferie.[23] Na obrázku 1.9 je zobrazen mikrokontrolér v pouzdře LQFP se 64 piny.



Obr. 1.9: NXP Kinetis K32L2B LQFP [23]

Módy napájení

Pro snížení příkonu výrobce doporučuje následující:

- Nastavit piny na známou hodnotu, pro řadu Kinetis je vhodnější ponechat volné piny „plovoucí“ a nastavit je na disabled
- Nastavit taktovací frekvence na co nejnižší hodnotu
- Snížení provozní teploty bude znamenat také nižší energetickou spotřebu
- Vypnout zdroj hodinového signálu u všech nepoužívaných modulů

Popis módů napájení

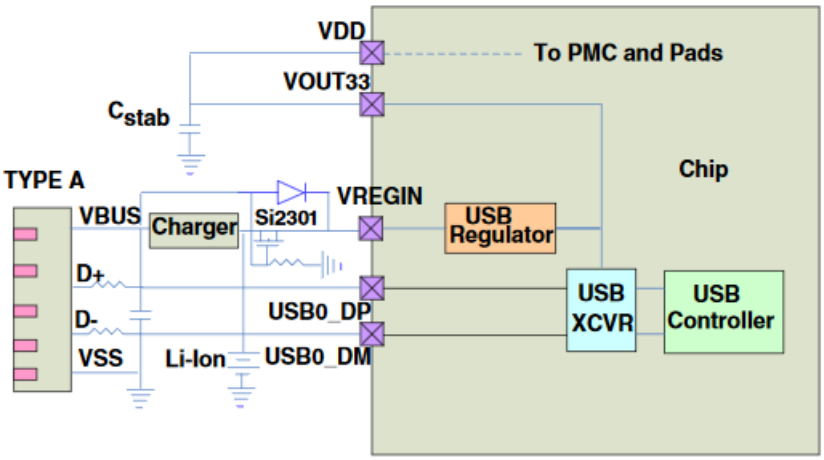
Mikrokontrolér Kinetis K32L2B disponuje několika módy běhu.

- **Run** - běžný mód, maximálný výpočetní výkon čipu. Nastane po každém resetu. Ukazatel na stack a programový čítač jsou nastaveny. Typický proudový odběr je 270 µA/MHz.
- **Wait** - je možné používat periferie, ale jádro ARM je uspané. Jednotka NVIC je připravena na žádost o přerušení (IRQ). Proudový odběr od 6,5 mA.
- **Stop** - nejnižší mód, který uchovává stav všech registrů. Jednotka NVIC je vypnutá, k probuzení z přerušení slouží AWIC. Hodinový signál k periferiím je zastaven. Jádro ARM je hluboce uspáno (deep sleep). Proudový odběr od 302 µA.
- **VLPR (Very Low Power Run)** - Napětový regulátor na čipu je v nízkopříkonovém módu, umožňuje běh jádra na snížené frekvenci 4 MHz a paměti Flash na frekvenci 1 MHz. Programování paměti Flash není dovoleno. Proudový odběr od 710 µA.
- **VLPW (Very Low Power Wait)** - Stejné jako VLPR, ale jádro je uspané. Proudový odběr od 450 µA.
- **VLPS (Very Low Power Stop)** - Nejnižší mód na kterém funguje převodník ADC a funkce přerušení z pinů. Hodinový signál k periferiím je zastaven, ale LPTIMER (Nízkopříkonový časovač), RTC (Hodiny reálného času), CMP (Komparátor) a TSI mohou být použity. Jednotka NVIC je vypnutá, k probuzení z přerušení slouží AWIC. Proudový odběr od 5,1 µA.
- **LLS (Low Leakage Stop)** - Jádro je hluboce uspáno (deep sleep). Hodinový signál k periferiím je zastaven. Periferie jsou v udržovacím stavu - paměť SRAM je napájena. LPTIMER (Nízkopříkonový časovač), RTC (Hodiny reálného času), CMP (Komparátor) a TSI mohou být použity. K probuzení slouží jednotka LLWU (Low-leakage wake up unit). Proudový odběr 2,1 µA až 10 µA.
- **VLLS3 (Very Low Leakage Stop3)** - Proudový odběr 1420 nA až 8 µA.
- **VLLS2 (Very Low Leakage Stop2)** - Proudový odběr 1420 nA až 4 µA.

- **VLLS1 (Very Low Leakage Stop1)** - LPTIMER (Nízkopříkonový časovač), RTC (Hodiny reálného času), CMP (Komparátor) a TSI mohou být použity. K probuzení slouží jednotka LLWU (Low-leakage wake up unit). Paměť SRAM není napájená. Je možné využít 32 bajtového systémového registru a 32 bajtového VBAT registru pro uložení kritických dat. Proudový odběr 690 nA až 2 µA.
- **VLLS0 (Very Low Leakage Stop0)** - Funkční jsou pouze jednotka LLWU a RTC. SRAM není napájená. Proudový odběr 190 nA až 300 nA.
- **BAT (Jenom záložní baterie)**

Napájení

Čip je možné napájet jedním Li-ion akumulátorem. Tolerance napájecího napětí je v rozmezí 1,71 až 3,6 V nebo je možné využít interního regulátoru napětí pro napájení z baterie nebo z USB, viz obr. 1.10.



Obr. 1.10: Napájení čipu přes USB [23]

1.4.2 OL2385

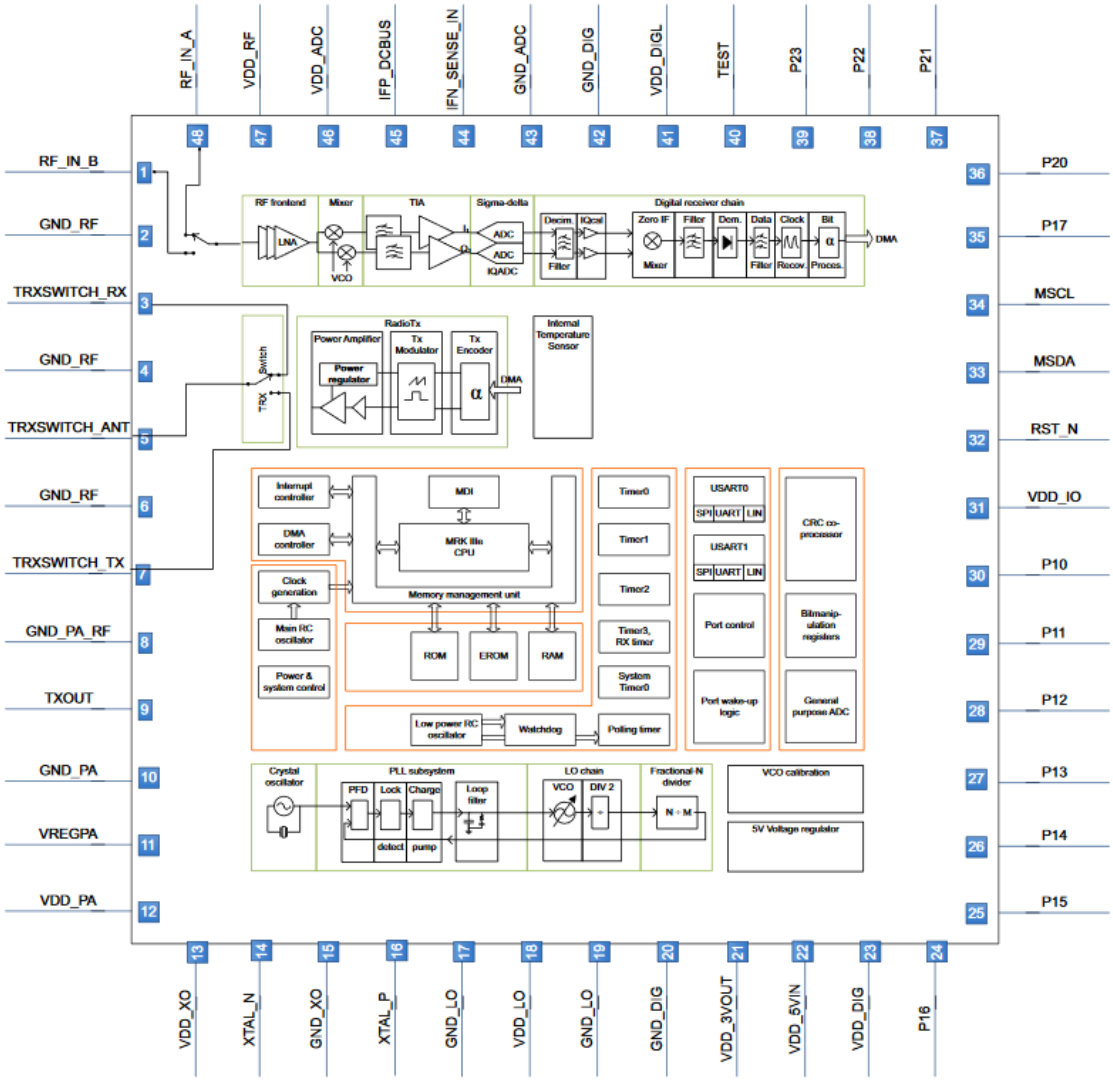
OL2385 je transceiver dodávaný firmou NXP pro průmyslové použití. Skládá se z běžně používaných bloků: krystalového oscilátoru, PLL (fázového závěsu) pro přesný výběr frekvence pro TX a RX, LNA (Low Noise Amplifier), nízkošumového zesilovače, atenuátoru pro automatické ovládání zisku (AGC), I/Q směšovače a dvou převodníků ADC s vysokým rozlišením.

Transceiver má zabudovaný RISC mikroprocesor, optimalizovaný pro vysoký výkon a nízkou spotřebu. Obsahuje také paměť typu EPROM pro zákaznické aplikace.

Součástí je také středně výkoný UHF vysílací systém s vysokým dynamickým rozsahem -35 dBm až +14 dBm, což je ideální pro úzkopásmové komunikační systémy. Maximální přenosová rychlost je 400 kbit/s NRZ.

Pro použití v aplikacích napájených bateriemi je možné využít několik časovačů pro buzení (wake-up) v daných intervalech. Buffery pro RX a TX se nachází v paměti RAM s autonomním DMA, což redukuje potřebný procesorový čas. Podpořená rozhraní jsou UART, SPI a LIN. Programování je možné realizovat pomocí HAL (Hardware Abstraction Layer).

Frekvenci nosné je možné nastavovat od 158 MHz až po 960 MHz, což umožňuje provoz v nelicencovaných pásmech po celém světě. Napájecí napětí lze volit v rozsahu od 1,9 V až po 5,5 V[14]. Na obrázku 1.11 je zobrazeno blokové schéma.



Obr. 1.11: Blokové schéma OL2385 [14]

InnoComm SN10-11

V době vypracování této semestrální práce (r. 2019), firma NXP nabízela ve spolupráci s firmou InnoComm Mobile Technology modul SN10-11 jako hotové řešení pro síť Sigfox, v rádiové konfiguraci RC1 certifikovanou Sigfoxem.

Modul InnoComm SN10-11 obsahuje RF transceiver NXP OL2385 doplněný o přizpůsobovací obvod, naladěný na rádiovou konfiguraci RC1 868 MHz. Je dodávaný se Sigfox firmwarem. K modulu je nutné připojit anténu laděnou na frekvenci 868 MHz. Impedance portu antény je 50 Ω. Na obrázku 1.12 je zobrazeno pouzdro čipu SN10-11.

Obr. 1.12: InnoComm SN10-11 [11]

Výběr vhodné antény

Anténu pro pásmo UHF 868 MHz je možné zakoupit u mnoha výrobců, například RF Solutions, Molex, Taoglas a další. Vyrábějí se buď v provedení dipólu s SMA konektorem nebo pro povrchovou montáž (SMT), či v ohebné nalepovací podobě. Na obrázku 1.13 je zobrazena vybraná anténa Molex.

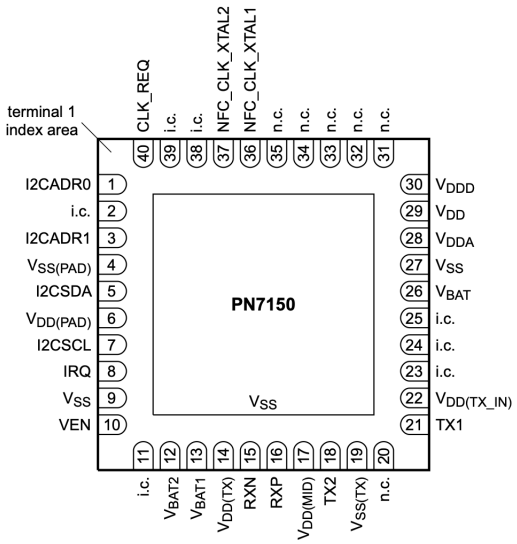
Obr. 1.13: Anténa Molex pro pásmo ISM 868 MHz s konektorem U.FL [30]

K příslušné anténě je také nutné vybrat odpovídající konektor.

1.4.3 PN7150

PN7150 je integrovaný obvod od firmy NXP Semiconductors určený pro NFC komunikaci. Podporuje několik operačních módů, např. čtečka (MIFARE, ISO/IEC 14443, Sony FeliCa), emulátor karty a přenosové módy NFC-IP. Modul je možné připojit k mikrokontroléru pomocí sběrnice I2C a protokolu NCI. Čip lze napájet přímo z akumulátoru a je možné využít dvou módů - standby a polling. Lze použít napájecí napětí v rozsahu 2,7 V až 5,5 V.

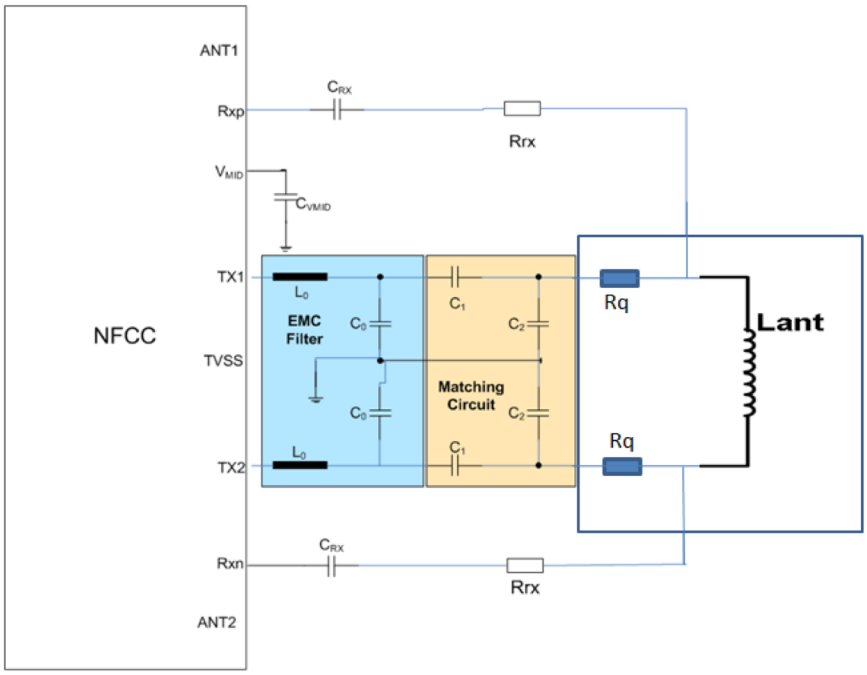
Jádro mikrokontroléru PN7150 je možné provozovat bez externího zdroje hodinového signálu (pouze s interním oscilátorem). Avšak pro použití s 13,56 MHz NFC je nutné připojit na pin XTAL1 externí oscilátor. Výrobce doporučuje použít externí krystal 27,12 MHz nebo externí zdroj hodinového signálu 13 MHz, 19,2 MHz, 24 MHz, 26 MHz, 38,4 MHz nebo 52 MHz. Na obrázku 1.14 je čip PN7150 v pouzdře HVQFN40.



Obr. 1.14: Pinout PN7150 v pouzdře HVQFN40 [20]

Anténa

Pro připojení antény je nutné zařadit přizpůsobovací obvod a EMC filtr. Obvyklá topologie takového obvodu je na obr. 1.15. EMC filtr se skládá z dolní propusti druhého řádu pro redukci spektrálního výkonu na vysokých frekvencích. C1 a C2 jsou použity k impedančnímu přizpůsobení na portech TX1 a TX2 (30 Ω) na frekvenci 13,56 MHz.



Obr. 1.15: Zapojení NFC antény [20]

Typická anténa pro použití v NFC je smyčková anténa. Charakteristika antény je definována počtem smyček, tloušťkou vedení, velikostí mezer mezi smyčkami a celkovou velikostí antény. Smyčkové antény mohou mít různé tvary, nejčastěji používané jsou obdélníkové a kruhové.

Další používané antény pro NFC jsou čipové induktory. Mezi jejich výhody patří menší velikost antény a dobrá účinnost v metalickém prostředí.

Přizpůsobení impedancí

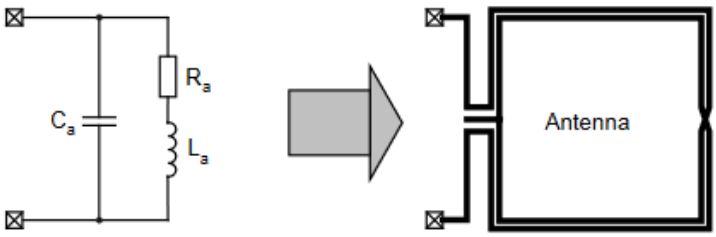
Impedanční přizpůsobení je situace, při kterém v obvodu nedochází k odrazu vln, ale naopak nastává maximální přenos energie ze zdroje do zátěže. Impedanční přizpůsobení je tedy stav, při níž činitelé odrazu zátěže a zdroje (generátoru) jsou komplexně sdruženy. Za této situace nedochází ke vzniku stojatého vlnění. [13]

Výpočet obvodu pro přizpůsobení PN7150 se provádí zvlášť pro operační mód čtečky a karty a děje se v pěti krocích. Zabývat se budeme pouze přizpůsobením pro režim čtečky podle [20].

1.5 Návrh NFC antény a přizpůsobovacího obvodu

1.5.1 Analýza antény a stanovení ekvivalentního obvodu

Prvním krokem je stanovení ekvivalentního obvodu antény. To je možné provést měřením na impedančním nebo vektorovém analyzátoru nebo výpočtem. Výstupem takové analýzy je sériový obvod RLC, viz obrázek 1.16.



Obr. 1.16: Sériový ekvivalentní obvod RLC [20]

Rezonanční frekvence obvodu f_0 by měla být vyšší jak 25 MHz. Je tedy třeba, aby parazitní kapacitance byla nízká. Z Thompsonova vztahu (1.1) lze odvodit následující vztah (1.2)

$$f_0 = \frac{1}{2\pi\sqrt{L_a C_a}} \tag{1.1}$$

$$C_a = \frac{1}{(2\pi f_0)^2 L_a} \tag{1.2}$$

K určení těchto elektrických ekvivalentních parametrů jsou doporučeny dvě metody.

- Měření na impedančním analyzátoru, jenž umožňuje změřit amplitudu a fázi impedance připojené antény.
- Měření na vektorovém analyzátoru

Činitel jakosti

Činitel jakosti antény závisí na hodnotách její induktance a sériové impedance. Jestliže je hodnota činitele jakosti Q příliš vysoká, pak je anténa selektivní. Rezonanční pásmo je tudíž příliš úzké a to může mít vliv na tvarování pulzů NFC signálu.

Firma NXP proto doporučuje, aby maximální hodnota činitele jakosti Q nepřekročila 35. Pokud je hodnota činitele jakosti vyšší, je možné použít tlumící rezistory zapojené v sérii na vstup antény, tzv. „damping“ rezistory.

Činitel jakosti antény je možné určit ze vztahu:

$$Q_a = \frac{\omega L_a}{R_a} \tag{1.3}$$

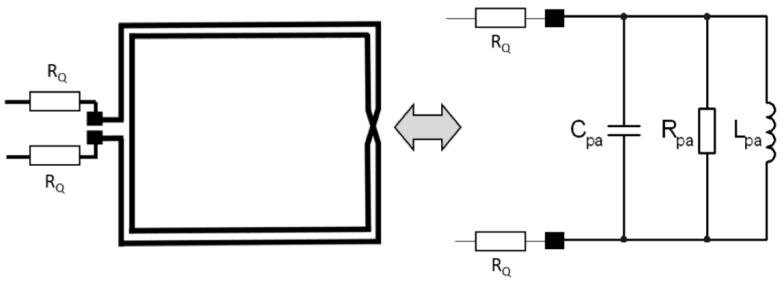
Výpočet tlumícího rezistoru pro dosažení činitele jakosti 35 zjistíme ze vzorce:

$$R_Q = 0,5 \left(\frac{\omega L_a}{35} - R_a \right) \tag{1.4}$$

Doporučená velikost činitele jakosti je v rozmezí 20 až 35.

Určení paralelního ekvivalentního obvodu

Paralelní ekvivalentní obvod antény (viz 1.17) s volitelně přidaným tlumícím rezistorem R_Q je zjištěn následným způsobem. L_{pa} je paralelní ekvivalentní indukčnost, C_{pa} paralelní ekvivalentní kapacita, R_{pa} paralelní ekvivalentní odpor.



Obr. 1.17: Paralelní ekvivalentní obvod RLC [20]

$$L_{pa} \hat{=} L_a \tag{1.5}$$

$$C_{pa} \hat{=} C_a \tag{1.6}$$

$$R_{pa} \hat{=} \frac{(\omega \cdot L_a)^2}{R_a + 2 \cdot R_Q} \tag{1.7}$$

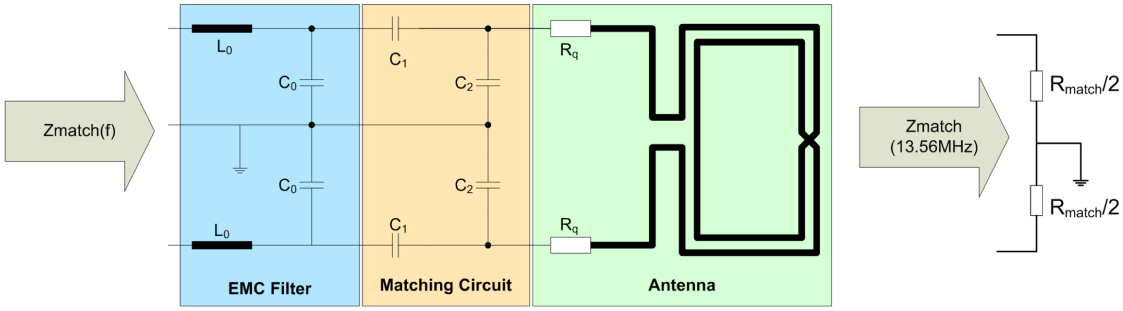
1.5.2 Návrh EMC filtru

EMC filtr pro PN7150 zastává dvě funkce: filtraci signálu a transformaci impedance.

Firma NXP doporučuje stanovit hodnotu L_0 v rozsahu od 270 nH do 1 µH a hodnotu rezonanční frekvence filtru f_r od 15,5 MHz do 17 MHz. Rezonanční frekvence EMC filtru musí být vyšší, než je hodnota frekvence nejvyšší subnosné. Hodnotu C_0 je nutné vypočítat ze vztahu 1.8

$$C_0 = \frac{1}{(2\pi f_r)^2 L_0} \tag{1.8}$$

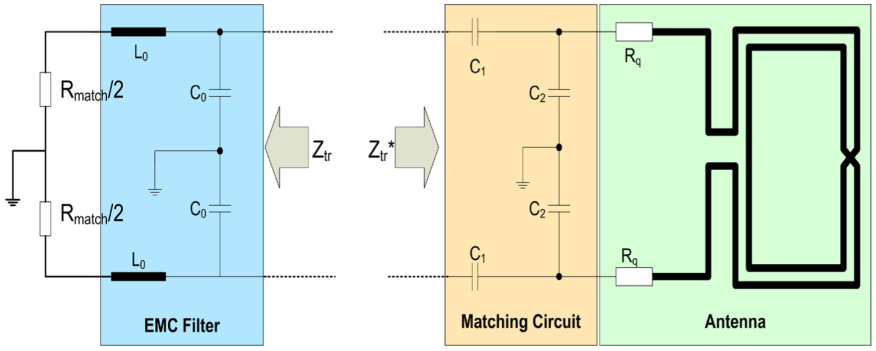
EMC filtr a přizpůsobovací obvod musí transformovat impedanci antény $Z_a(f)$ na impedanci Rm na frekvenci $f = 13,56$ MHz.



Obr. 1.18: Transformace impedance [20]

Změřená impedance $Z_m(f)$ může být modelována jako ekvivalentní obvod zatěžující každý TX pin $R_{match}/2$ na frekvenci $f = 13,56$ MHz. To je zobrazeno na obr. 1.18.

„Rozpůlením“ obvodu za EMC filtrem a s využitím předpokladu $R_{match}/2$ můžeme spočítat hodnoty C1 a C2 viz obr. (1.19).



Obr. 1.19: Definice transformace impedance Z_{tr} [20]

$$Z_{tr} = R_{tr} + jX_{tr} \tag{1.9}$$

$$Z_{tr}* = R_{tr} - jX_{tr} \tag{1.10}$$

$$R_{tr} = \frac{R_{match}}{(1 - \omega^2 \cdot L_0 \cdot C_0)^2 + \left(\omega \cdot \frac{R_{match}}{2} \cdot C_0\right)^2} \tag{1.11}$$

$$X_{tr} = 2 \cdot \omega \cdot \frac{L_0 \cdot (1 - \omega^2 \cdot L_0 \cdot C_0) - \frac{R_{match}^2}{4} \cdot C_0}{(1 - \omega^2 \cdot L_0 \cdot C_0)^2 + \left(\omega \cdot \frac{R_{match}}{2} \cdot C_0\right)^2} \tag{1.12}$$

C1 a C2 jsou v kombinaci s EMC filtrem použity k naladění antény na 13,56 MHz pro danou hodnotu impedance R_{match}. Pro čip PN7150 je doporučována hodnota 30 Ω.

Pro výpočet hodnoty C1 a C2 platí.

$$C_1 \approx \frac{1}{\omega \cdot \left(\sqrt{\frac{R_{tr} \cdot R_{pa}}{4}} + \frac{X_{tr}}{2}\right)} \tag{1.13}$$

$$C_2 \approx \frac{1}{\omega^2 \cdot \frac{L_{pa}}{2}} - \frac{1}{\omega \cdot \sqrt{\frac{R_{tr} \cdot R_{pa}}{4}}} - 2 \cdot C_{pa} \tag{1.14}$$

Na základě spočítaných hodnot by výsledná impedance $Zmatch = Rmatch + jXmatch$ měla být změřena na impedančním nebo vektorovém analyzátoru mezi piny TX1 a TX2.

1.5.3 Návrh antény

Komunikace v NFC probíhá na frekvenci 13,56 MHz a pro anténu se běžně využívá indukční smyčka. Vazba mezi přijímačem a vysílačem je tedy induktivní. Funguje pouze na velmi krátkou vzdálenost, obvykle jen do 4 cm. Nejedná se tedy o typickou anténu. Jak již bylo zmíněno, anténa je charakterizována především počtem smyček, vzdáleností mezi smyčkami, tloušťkou měděné vrstvy a celkovou plochou, kterou anténa zabírá.

Indukčnost antény bude závislá především na počtu smyček a ploše antény. Zjednodušeně řečeno, čím je větší indukčnost, tím bude lepší indukční vazba mezi přijímačem a vysílačem. Ovšem s větší plochou antény a počtem smyček vzrůstá i odpor a parazitní kapacita antény a též ladění představuje větší problém. Je tedy nutné tyto parametry optimalizovat. Dle doporučení firmy NXP se má indukčnost antény pohybovat kolem 1μH, což pro anténu o rozměrech 65 × 65 mm představuje dvě smyčky.[5]

Doporučené parametry firmou NXP pro čip NFC PN7150 najdeme v tabulce 1.4.

Popis	**Minimum**	**Maximum**
Plocha	500 mm^2	5000 mm^2
Počet smyček	2	8
Šířka cesty	0,2 μH	2 mm
Mezera mezi smyčkami	0,2 μH	2 mm
Tloušťka mědi	20 μm	

Tab. 1.4: Doporučené parametry NFC antény [20]

Pro výpočet indukčnosti čtvercové antény se dá využít zjednodušený vzorec 1.15 (převzato z ST Microelectronics).[6]

$$L_{ant} = 2,34 \cdot \mu_0 \cdot N^2 \frac{d}{1 + 2,75p} \tag{1.15}$$

Kde:

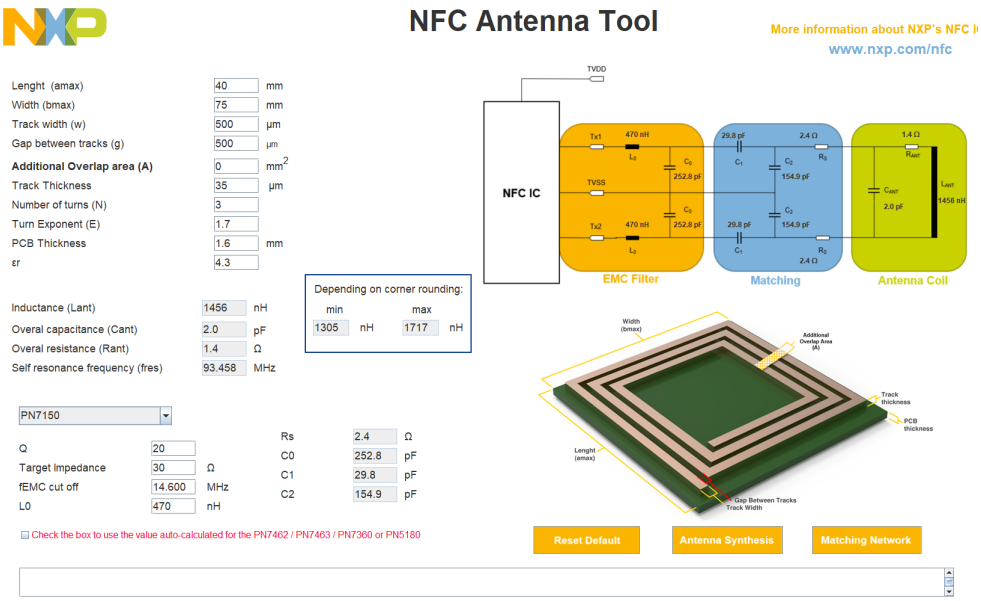
$d = (d_{out} + d_{in})/2$

$p = (d_{out} - d_{in})/(d_{out} + d_{in})$

d_{out}: vnější rozměr antény

d_{in}: vnitřní rozměr antény

Pro návrh antény je také možné využít nástroje NFC Antenna Tool [5], který umí spočítat hodnoty součástek pro přizpůsobovací obvod a EMC filtr na základě zadaných rozměrů antény. Viz obr. 1.20.



Obr. 1.20: NFC Antenna Tool [5]

Ze získaných rozměrů je možné navrhnout anténu například ve webovém nástroji „Simple rectangular spiral footprint generator“ vytvořený Konradem Beckmannem. Výstupem generace je obrázek 1.21 ve formátu PNG, který je možné převést na footprint, například nástrojem bitmap2component, jenž je součástí návrhového software KiCad.

Parametry vygenerované antény byly spočítané pomocí NFC Antenna Tool. Najdeme je v tabulce 1.5. Zvolené hodnoty součástek pro přizpůsobovací obvod najdeme v tabulce 1.6.

Obr. 1.21: Generovaná NFC anténa 75x40 mm

Parametr	**Hodnota**
Délka [mm]	40
Šířka [mm]	75
Šířka cesty [mm]	0,5
Mezera mezi cestami [mm]	0,5
Tloušťka mědi [μm]	0,35
Počet smyček	3
Tloušťka PCB [mm]	1,6
Permitivita substrátu	4,3
Indukčnost antény [nH]	**1456**
Kapacita antény [pF]	**2**
Odpor antény [Ω]	**1,4**

Tab. 1.5: Parametry antény

Parametr	**Vypočtená hodnota**	**Zvolená hodnota**
L_0	470 nH	470 nH
R_s	2,4 Ω	2,4 Ω
C_0	252,8 pF	250 pF
C_1	29,8	30 pF
C_2	154,9 pF	150 pF || 5 pF

Tab. 1.6: Vypočtené hodnoty součástek

1.6 Displej

K zobrazování informací o udělení, či neudělení přístupu a také jestli je zámek odemčený je použit displej. Displej je možné využít též jako ukazatel stavu nabití akumulátoru. K připojení displeje je vyvedeno pět pinů přímo na desce. Lze tak využít téměř libovolný displej komunikující po sběrnici SPI.

1.6.1 Waveshare e-paper 2.13 V2

Vzhledem ke snaze minimalizovat spotřebu elektrické energie navrhovaného zařízení byl vybrán displej typu elektronický papír. Displej je schopný uchovávat zobrazený text či obrázky bez spotřeby elektrické energie. El. energie je potřeba pouze k překreslení.

Displej Waveshare e-paper 2.13 V2 je zobrazovací jednotka typu elektronický papír (elektroforetický displej s aktivní matricí – AMEPD). Displej se vyrábí ve dvoubarevné a tříbarevné variantě – v tomto případě se jedná o dvoubarevnou variantu BW, tedy černá a bílá. Rozlišení displeje je 250x122 pixelů. Displej komunikuje pomocí rozhraní SPI. Existují dvě nekompatibilní varianty V1 a V2, na to je třeba myslet při vývoji ovladače. Na obrázku 1.22 je displej včetně HAT desky.

Obr. 1.22: Waveshare displej [31]

1.7 Ovládání zámku dveří

Pro konstrukci elektronicky ovládaných dveří se zpravidla využívají tři principy

- Elektromotorické zámky
- Elektromechanické zámky
- Elektromagnetické zámky

Elektromagnetické zámky obsahují elektromagnet, který svoji silou drží dveře v zamčené poloze. Elektromagnet musí být neustále napájen. Tento typ zámku není tedy vhodný pro bateriovou aplikaci.

Elektromechanické zámky se odblokují při přivedení napětí na cívku, která k sobě přitáhne jazýček a uvolní střelku.

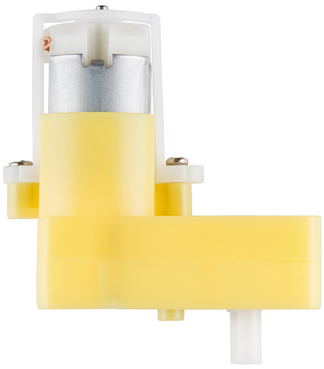
Elektromotorické zámky používají elektromotor k ovládání zámku. Z důvodu kompatibility z běžnými dveřmi se zadlabacím zámkem a také z důvodu nízké ceny byl zvolen elektromotorický způsob ovládání zámku.

K ovládání zámku dveří je použit stejnosměrný motor ovládaný přes H-můstek NXP MPC17531. Motor ovládá přímo cylindrickou vložku, která je pro tento účel upravena.

1.7.1 Stejnosměrný motor

Stejnosměrný motor je definován jako točivý stroj napájený stejnosměrným proudem. Přepólováním napájecího napětí lze tedy docílit změnu smyslu otáčení motoru. Rychlost otáček motoru lze regulovat změnou napájecího napětí, nicméně obvykle je to realizováno pomocí PWM. Pro řízení tohoto motoru lze využít H můstek.

Na obrázku 1.23 je vybraný motor pro ovládání zámku. Výrobcem motoru je Sparkfun Electronic, motor je prodáván pod označením ROB-13258. Motor je dodáván včetně úhlové plastové převodovky s převodovým poměrem 1:48. Motor je možné napájet od 3 do 6 V. Klidový proud bez zátěže je maximálně 170 mA. Maximální proudový odběr (stall current) při 3 V je 1,5 A.

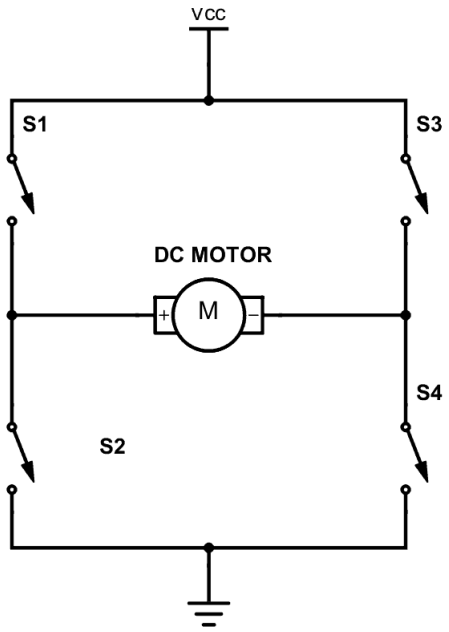


Obr. 1.23: Motor pro ovládání zámku ROB-13258 [38]

1.7.2 H Můstek

H můstek je elektrický obvod pro řízení stejnosměrných motorů. Pro řízení bipolárních krokových motorů je možné využít dva H můstky, někdy také označovaný jako dvojitý H můstek. Tyto obvody je možné použít pro řízení jednoho krokového motoru, nebo dvou stejnosměrných motorů. Na obrázku 1.24 je zjednodušené schéma H

můstku, který ovládá stejnosměrný motor. Pokud je spínač 1 a spínač 4 v sepnutém stavu a spínače 2 a 3 v rozepnutém, motor se otáčí jedním směrem. Pro otáčení motoru v druhém směru je nutné sepnout spínače 2 a 3 a rozepnout spínače 1 a 4. Spínače jsou většinou realizovány pomocí tranzistorů MOSFET nebo bipolárních tranzistorů.

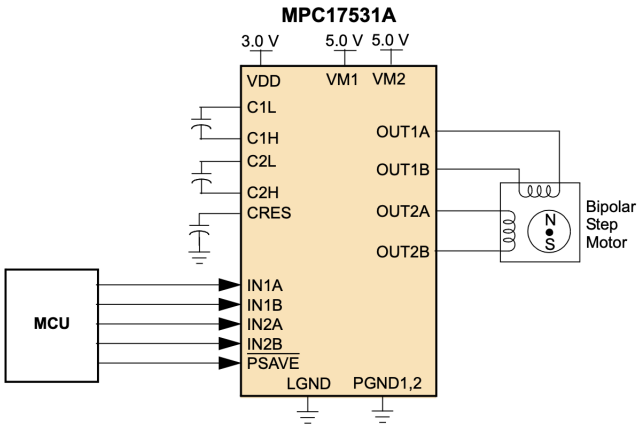


Obr. 1.24: Princip funkce H můstku [32]

1.7.3 MPC17531A

NXP MPC17531A je monolitický duální H můstek pro řízení krokových nebo stejnosměrných motorů. Vstupní napájecí napětí je od 2 do 8,6 V. Je využívána proudová pumpa.

Motory je možno nezávisle řídít pomocí PWM až do frekvence 200 kHz. MPC17531A má čtyři módy běhu: dopředu, dozadu, brzda a stav vysoké impedance. Maximální proud pro jeden motor je 700 mA v kontinuálním režimu a 1,4 A špičkově. Na obrázku 1.25 je zjednodušené zapojení H můstku.

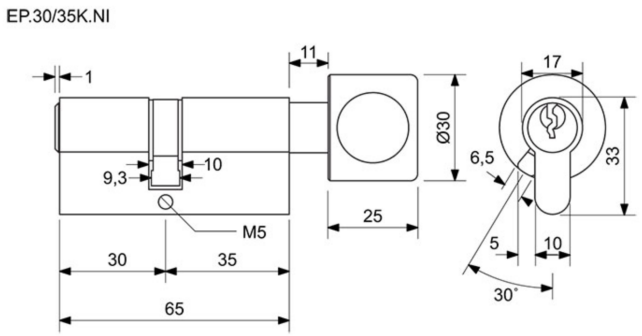


Obr. 1.25: Duální H můstek MPC17531A [18]

1.8 Zámek

Pro účely demonstrace funkčnosti byla vybrána stavební cylindrická vložka s otočným knoflíkem Richter Czech EP.30/35K.NI. Tato vložka není příliš vhodná pro zabezpečení objektu, protože je certifikována pouze jako stavební. Pro účely demonstrace funkce zařízení však postačí. Na obrázku 1.26 je nákres této cylindrické vložky.

Cylindrická vložka byla upravena tak, že byl sejmut otočný knoflík a na místo něj bylo instalováno ozubené kolo k motorickému ovládání. Na hřídel motoru je rovněž instalováno ozubené kolo. Převodový poměr tohoto ústrojí je cca 1:4. Cylindrická vložka byla osazena do standardního zadlabacího zámku. Zámek byl umístěn do upravených zmenšených dveří, které byly vyrobeny ze standardních interiérových dveří. Fotografie dveří je v příloze.

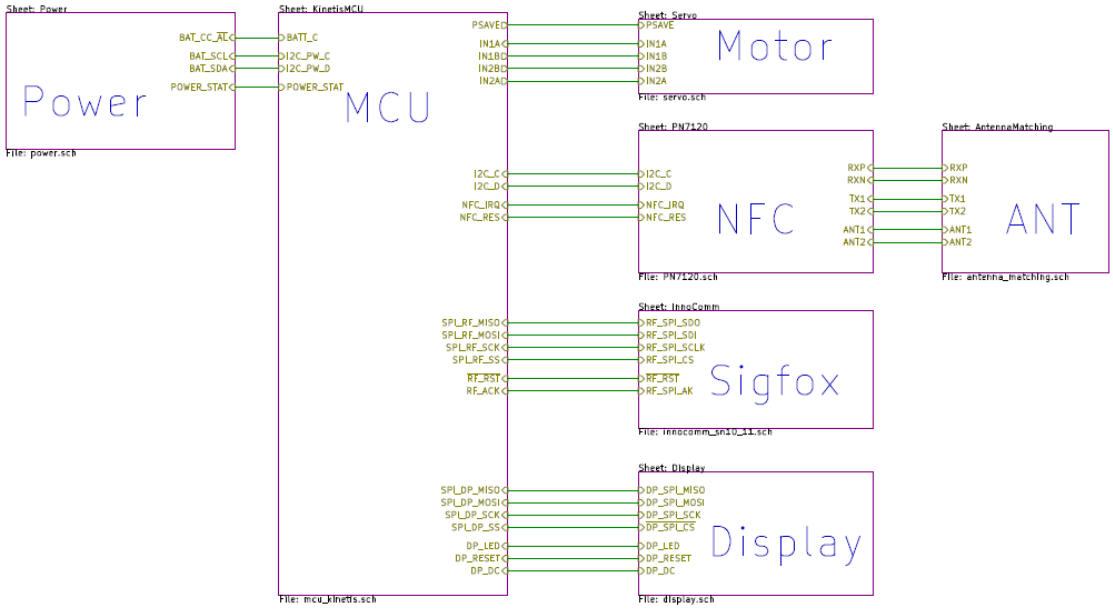


Obr. 1.26: Cylindrická vložka Richter EP.30/35K.NI [35]

2 Návrh zapojení

Tato kapitola popisuje návrh desky plošných spojů. Postupuje od schematického návrhu po návrh layoutu.

K návrhu schématu byl použit software KiCad. Program Eeschema, jenž je součástí KiCadu, umožňuje vytvoření hierarchického návrhu. Rozdělením do dílčích bloků se stává výsledný návrh přehlednější.



Obr. 2.1: Hierarchický schématický návrh

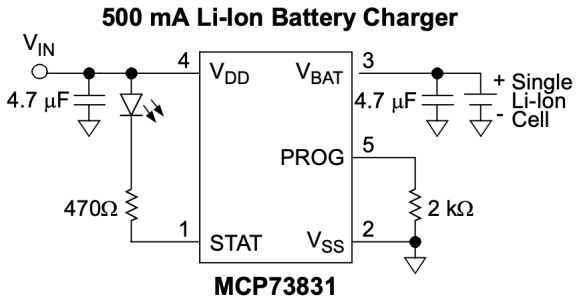
Hierarchický návrh obsahuje bloky pro mikrokontrolér (MCU), napájení (Power), NFC, Sigfox, řízení motoru, displej (Display) a anténu spolu s odrušovacími a přizpůsobovacími obvody (ANT).

2.1 Napájení

Zařízení je vhodné napájet bateriově, nejlépe pomocí Lithium-iontových akumulátorů. K hlavním výhodám těchto akumulátorů patří velmi vysoká hustota energie cca 200 Wh/kg, velmi nízký samovybíjecí proces, vysoké nominální napětí 3,7 V a velký počet nabíjecích cyklů (cca 500 až 1000). Mezi nevýhody uveďme například stárnutí těchto akumulátorů a složitější proces jejich nabíjení [28].

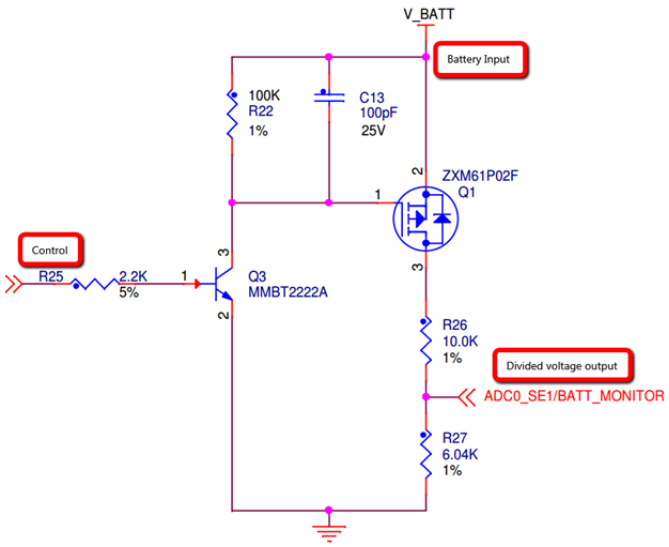
Mezi průmyslově nejpoužívanější lithium-iontové akumulátory patří cylindrický článek 18650 s obvyklou kapacitou 1500-3500 mAh a rozměrech 65x18 mm [27].

Dobíjení akumulátoru je možné realizovat například prostřednictvím USB a obvodu pro nabíjení baterie Microchip MCP73831 (2.2). Tento jednoduchý, miniaturní obvod umožňuje dobíjet články typu Li-ion konstantním proudem, jehož velikost se jednoduše nastaví pomocí rezistoru.



Obr. 2.2: Typická aplikace MCP73831 [17]

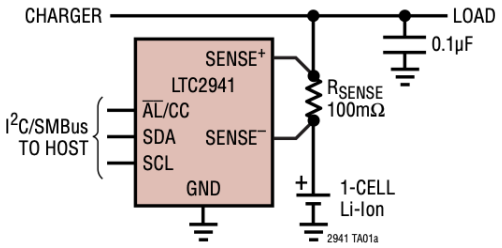
Obvod nabíjení je také vhodné doplnit obvodem pro monitoring baterie. Pokud bychom požadovali pouze měřit hodnotu napětí baterie, je to možné realizovat pomocí AD převodníku a děliče napětí a lze tak přímo využít periferii na mikrokontroléru, viz obr. 2.3.



Obr. 2.3: Měření napětí na baterii pomocí ADC

Pokročilejší řešení pro monitoring baterie sestává z obvodů pro měření náboje, který baterií protekl. Takové obvody dokáží stav baterie zhodnotit velmi přesně. Ke komunikaci s řídicí jednotkou (mikrokontrolérem) se většinou používá sběrnice I2C. Zařízení jako je chytrý zámek vyžaduje spolehlivý zdroj napájení a také je nutné

včas upozornit uživatele, že stav nabití je nízký, tak aby nedošlo k situaci, že zámek bude nefunkční. Bude tedy vhodnější využít obvod pro monitoring baterie, například LTC2941 na obr. 2.4.



Obr. 2.4: LTC2941 Typická aplikace [15]

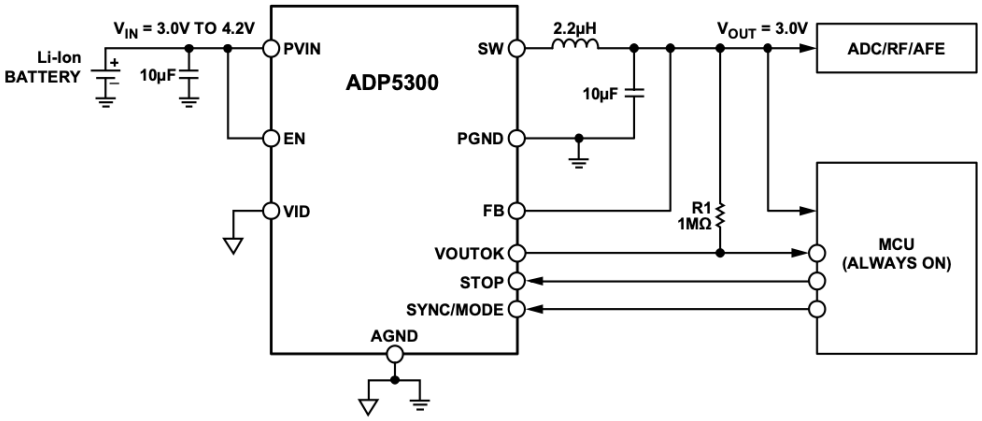
Dalším nezbytným obvodem při napájení z baterie je regulátor napětí, vzhledem k tomu, že většina mikroprocesorů a logických obvodů operuje na úrovni 3,3 V. Dají se použít jak lineární regulátory napětí tak spínané regulátory napětí. Spínané regulátory jsou zpravidla účinější, jejich účinnost se pohybuje kolem 90%, zatímco účinnost lineárních regulátorů je závislá na poměru vstupního a výstupního napětí a zpravidla bývá účinost menší než u spínaného regulátoru [8].

Zejména pro bateriové aplikace je také nutné zvážit proudový odběr samotného regulátoru. Například spínaný regulátor Analog Devices ADP5300 (2.5) má velmi nízký klidový odběr (quiescent current) až 180 nA v režimu hystereze. Nevýhodou spínaných regulátorů je vysokofrekvenční rušení, které můžou vnášet do obvodu.

V případě lineárních regulátorů pro bateriové aplikace je nutné se zaměřit na klidový proudový odběr (ultra low quiescent current) a také na nízký úbytek napětí (low dropout voltage), protože zařízení bude napájeno z lithiové baterie a při vysokém úbytku napětí by se baterie nemohla plně vybít (do 2,7 V). Například regulátory z rodiny Texas Instruments TPS783 dosahují velmi dobrých parametrů pro bateriové aplikace.

Vzhledem k použití vysokofrekvečních obvodů (Sigfox a NFC) bude lepší využít lineární regulátor. Spínaný regulátor by mohl do obvodu vnášet nežádoucí vysokofrekvenční rušení.

Požadavky na napájení byly získány z katalogových listů jednotlivých součástí a na základě těchto údajů byly stanoveny dvě napájecí větve 3V0 a VBAT, viz tabulka 2.1. Větev 3V0 (3 V) je výstupem z napěťového regulátoru a VBAT je výstup z akumulátoru. Napětí na akumulátoru se pohybuje od 2,7 V po 4,2 V při plně nabitém stavu. Větev 3V0 je využita pro napájení hlavního mikrokontroléru, digitální části NFC kontroléru, Sigfox modulu a displeje. Celkový maximální proudový odběr větve



Obr. 2.5: Spínaný regulátor ADP5300 [16]

Část	**Označení**	U_{min}	U_{max}	I_{max}	I_{typ}	$I_{standby}$	**Větev**
Jednotka		V	V	mA	mA	μA	-
MCU	K32L2B	1,71	3,6	15	5	1.3	3V0
NFC	PN7150 (digital)	3	3,6	15	-	-	3V0
NFC	PN7150 (battery)	2,7	5,5	190	0,15	150	VBAT
Sigfox	SN10-11	2,5	3,6	30	10	2,5	3V0
LDO	TPS783	2,2	5,5	0,008	0,001	0,8	VBAT
Nabíjení b.	MCP73831	3,75	6	1.5	0,053		VBAT
Monitor b.	LTC2941	2,7	5,5	0,1	0,07	70	VBAT
Displej	Waveshare 2.13	2,2	3,7	4,5		2	3V0
H můstek	MPC17531A	2,7	3,6	3,7		1	3V0
Motor		2,7	6	1500	170	1	VBAT

Tab. 2.1: Požadavky na napájení jednotlivých komponent

3V0 je 70 mA. Vzhledem k maximálnímu proudovému odběru bude dostatečné využít lineární regulátor TPS78330 s výstupním proudem 150 mA (maximálně špičkově 400 mA).

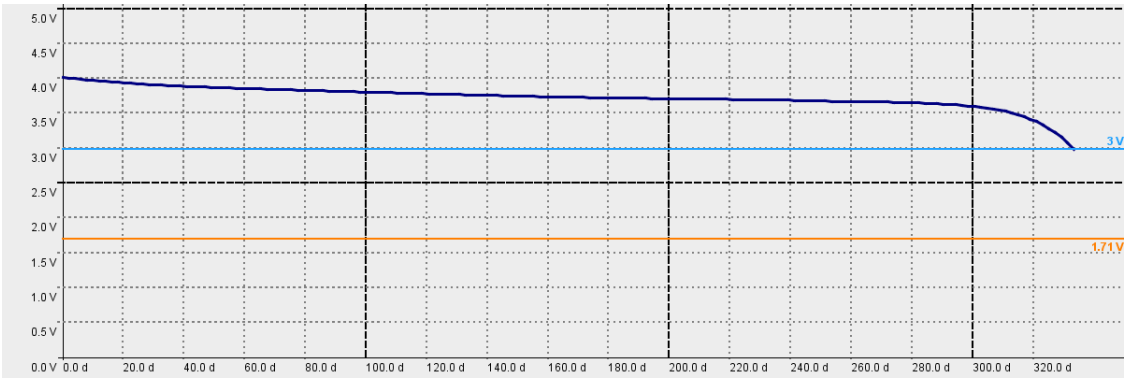
2.1.1 Simulace provozu na baterii

K simulaci byl použit nástroj MCU Power Estimation Tool od NXP (Freescale). Simulován byl provoz mikrokontroléru MKL43, který je téměř identický jako K32L2B (v době psaní práce nebyl K32L2B podpořen). Jako baterie byl zvolen lithium-iontový článek o nominálním napětí 3,7 V a kapacitě 3000 mAh, který byl vybíjen po 2,7 V. Do simulace bylo zahrnuto pět stavů, které se cyklicky opakovaly viz tab.

2.2. Čas jednoho cyklu je 2 h a 8 sekund. Průměrná spotřeba je 372 µA a při této spotřebě by výdrž baterie byla zhruba 333 dní viz tabulka 2.2 a obr. 2.6

#	Stav	Doba	Režim	Jádro	Flash	Odběr jádra	Celkový proud
1	NFC_Poll	2 h	LLS	OFF	OFF	2.06 µA	252.66 µA
2	Wakeup	10 µs	Run	8 MHz	4 MHz	1.92 mA	2.12 mA
3	Tag_read	2 s	Run	8 MHz	4 MHz	1.92 mA	2.9 mA
4	Unlock	4 s	Run	8 MHz	4 MHz	1.92 mA	202.7 mA
5	MSG_send	2 s	Run	8 MHz	4 MHz	1.92 mA	22.7 mA

Tab. 2.2: Simulace běhu z baterie



Obr. 2.6: Graf simulace vybíjení baterie

2.2 Mikrokontrolér

Mikrokontrolér K32L2B je napájen z větve 3V0. Pro testovací účely je možné jej také napájet přes interní lineární regulátor z baterie. Z toho důvodu je před pinem VREGIN umístěn pájitelný jumper. Mikrokontrolér je programován přes rozhraní SWD, které je vyvedeno na standardní desetipinový konektor.

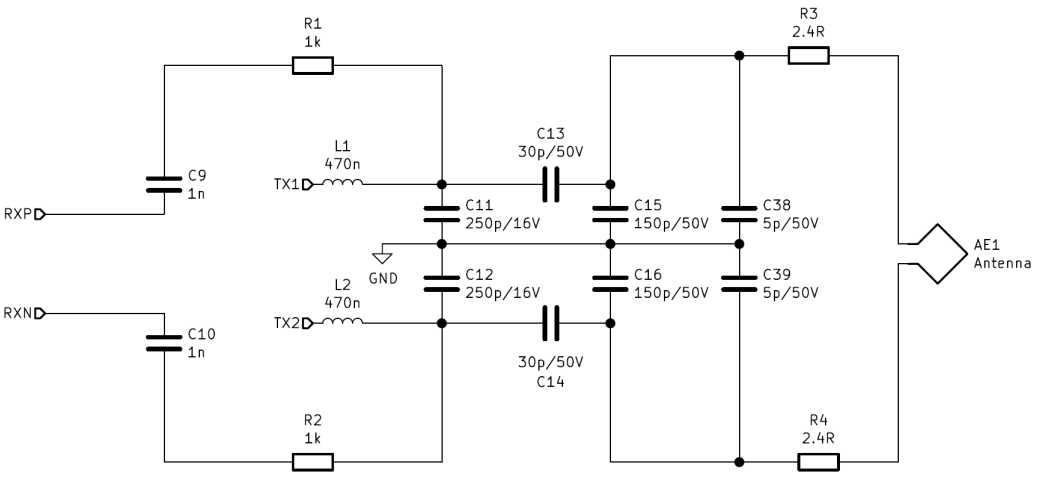
2.3 NFC

NFC čip PN7150 má RF část napájenou z baterie (napájen je interní lineární regulátor). Digitální část je napájena z větve 3V0. K čipu je připojen krystal 27,12 MHz pro generování přesného hodinového signálu potřebného pro NFC komunikaci. Čip je s mikrokontrolérem spojen pomocí rozhraní I2C, přes resetovací pin a přes

pin pro přerušení. Pin pro přerušení je vyveden do jednotky probuzení (LLWU) na mikrokontroléru. Pro sběrnici I2C jsou vyvedeny testovací body.

2.3.1 Přizpůsobovací obvod a EMC filtr

Hodnoty součástek byly zvoleny podle tabulky 1.6. Při návrhu DPS je vhodné součástky umístit symetricky. Kritickou částí návrhu je zvolit vhodnou cívku, která má hodnotu Q větší jak 20 na frekvenci 13,56 MHz, rovněž je vhodné cívky neumisťovat paralelně vedle sebe tak, aby nevznikl transformátor. Paralelní kondenzátor C15/C16 je zdvojený, tak aby bylo možné dosáhnout lepšího naladění. Schéma navrženého přizpůsobovacího obvodu je na obrázku 2.7.



Obr. 2.7: Schéma navrženého přizpůsobovacího obvodu

2.4 Sigfox

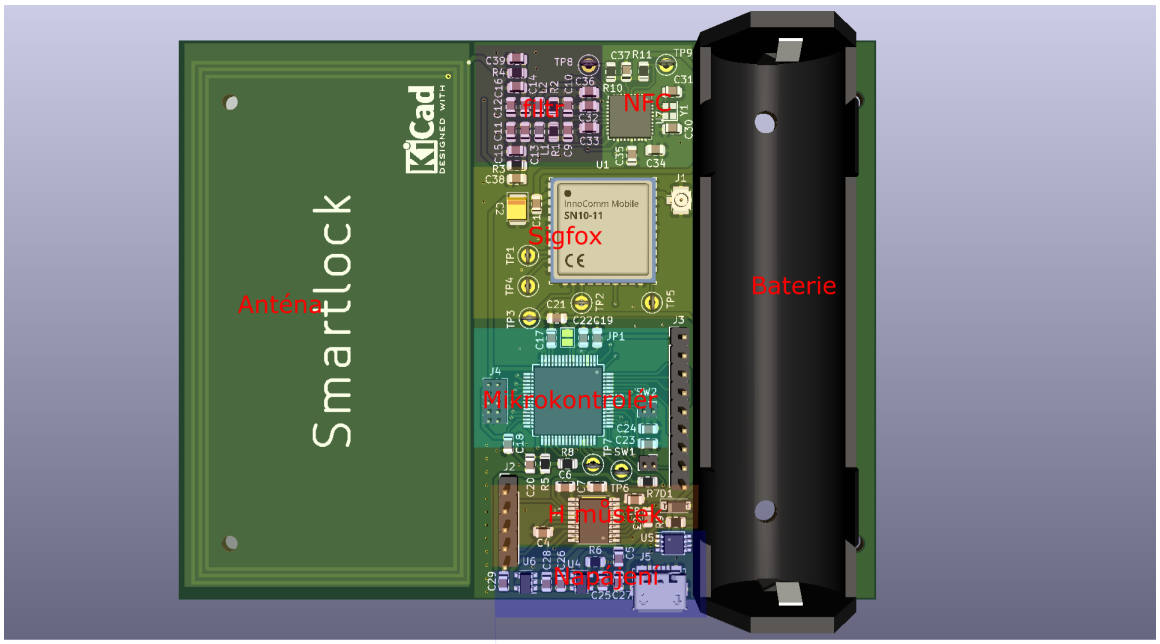
Modul InnoComm SN10-11 je napájen z větve 3V0. Blokování napájení je řešeno dle doporučení výrobce kondenzátorem 47 µF (použit je tantalový kondenzátor 10 V) a 33 pF. Jako konektor na anténu je použit Hirose U.FL. Čip je s mikrokontrolérem spojen pomocí dedikovaného rozhraní SPI a po stranách čipu jsou vyvedeny testovací body pro účely měření.

2.5 H můstek

H můstek je napájen z baterie přes zenerovu diodu, která obvod chrání před indukčními špičkami, které mohou nastat při řízení motoru. Připojení motoru je řešeno přes pětipinový konektor.

2.6 Deska plošných spojů

Deska plošných spojů byla navržena v programu Pcbnew, který je součástí sady KiCad. Je navržena ve třídě přesnosti 6 ve dvou vrstvách. Rozměry desky jsou 100x80 mm. Na desce se nachází montážní otvory pro šrouby M2. Součástí desky jsou také montážní otvory pro pouzdro na baterii 18650. Na obou stranách DPS je rozlita měď jako zemní plocha (GND). Jednotlivé části navržené desky plošných spojů jsou popsány na obrázku 2.8. Na obrázku 2.9 je vyrenderovaný pohled na DPS s využitím metody sledování paprsku (ray tracing).



Obr. 2.8: Popis jendotlivých částí DPS

Obr. 2.9: Pohled na DPS

3 Firmware

Tato kapitola se zabývá návrhem a optimalizací firmwaru pro mikrokontrolér, který bude zprostředkovávat komunikaci s modulem pro síť Sigfox a modulem pro NFC. Je nutné aby firmware řídil uspávání a probouzení mikrokontroléru. Další úlohou firmwaru je řízení přístupu, je tedy třeba definovat databázi uživatelů, kteří budou mít přístup.

3.1 Hlavní program

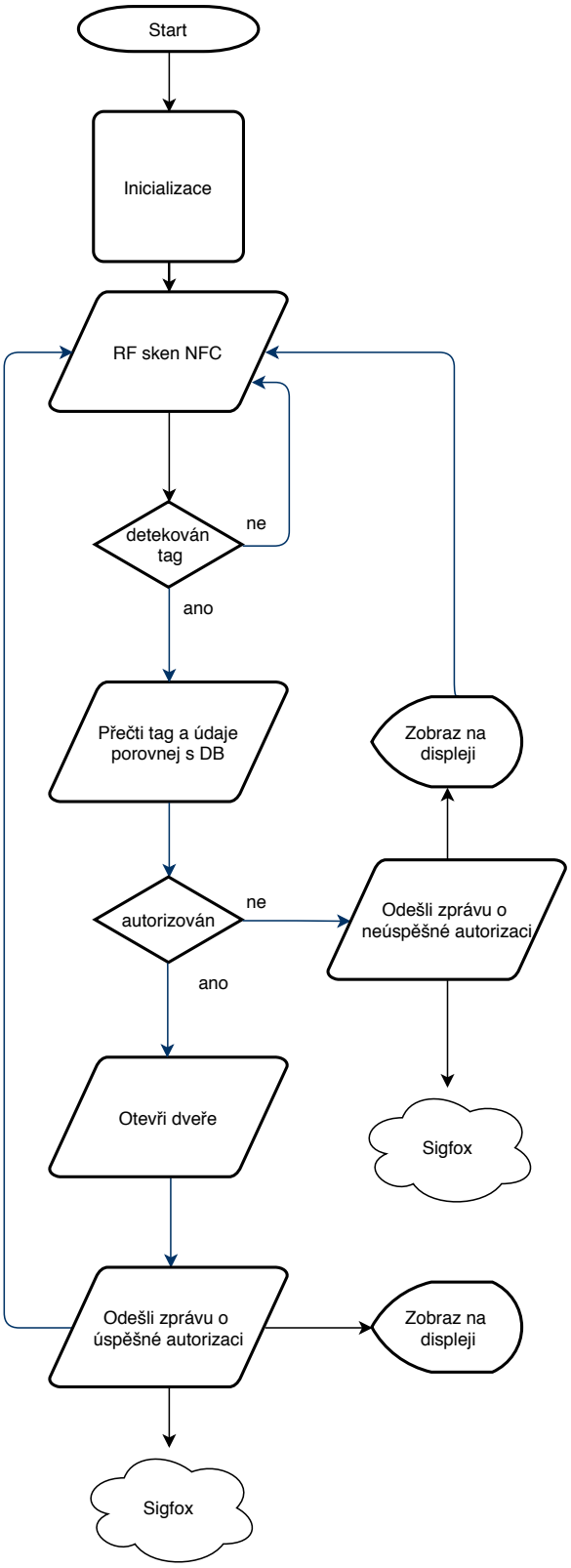
Po inicializaci pinů, hodin a periferií se inicializuje komunikace s modulem Inno-Comm SN10-11 a s displejem Waveshare. Jsou vyčteny informace o zařízení Inno-Comm a je zaslána inicializační zpráva do sítě Sigfox. Poté se zavolá funkce *task_nfc*, kde se sestaví komunikace s NFC modulem a započne se s vyhledáváním NFC tagů. V době čekání na přerušení se hlavní mikrokontrolér uspí. Pokud je nalezen NFC tag, tak se vygeneruje přerušení a probudí se hlavní mikrokontrolér a provede se proces autentizace použitého NFC tagu.

Nejprve se ověří zda je identifikátor tagu UID v databázi a pokud ano, tak se zahájí šifrovaná komunikace s tagem pomocí tajného klíče. Poté se přečte klíč, který je uložený v NFC tagu v sektoru 1 v paměťovém bloku 4. Pokud klíč i UID odpovídá databázi, tak se odešle zpráva do sítě Sigfox, která obsahuje informaci o tom zda došlo k odemčení či zamčení zámku.

Na obrázku 3.1 je znázorněn vývojový diagram hlavního programu. V tabulce 3.1 jsou popsány hlavní zdrojové soubory.

Modul	**Popis**
main.c	Hlavní modul obsahující vstupní bod
nfc_task.c	Obsluha NFC modulu a čtení tagů
sigfox.c	Obsluha odesílání zpráv do sítě Sigfox
power_mode_switch.c	Obsluha a přepínání úsporných režimů
user	Databáze uživatelů a NFC tagů
display	Vypisování zpráv na displeji

Tab. 3.1: Hlavní zdrojové soubory



Obr. 3.1: Vývojový diagram

3.2 Úsporný režim

Vzhledem k požadavku na nízkou energetickou spotřebu zařízení je nutné, aby komunikace mezi jednotlivými moduly probíhala pomocí přerušení a také aby čas v módu běhu byl co nejnižší a čas v režimu spánku co nejvyšší. Nejvýhodnější z hlediska spotřeby je režim VLLS0, u kterého se spotřeba pohybuje okolo několika stovek nanoampérů. V tomto režimu je aktivní pouze jednotka pro probuzení (LLWU). Nevýhodou tohoto režimu je reset mikrokontroléru po probuzení. Nejúspornější režim, který zachovává stav aplikace je režim LLS (Low leakage stop). O probuzení (přechod do režimu RUN či VLPR) z těchto režimů spánku se stará jednotka LLWU (low leakage wake up unit) a jako impulz k probuzení může sloužit nástupná či sestupná hrana na pinu GPIO, nebo přetečení úsporného časovače (LPTMR). Je tedy nutné nejprve nadefinovat události, které povedou k probuzení mikrokontroléru tj. přechod do režimu běhu, viz tab. 3.2.

Před přechodem do úsporných režimů je ještě vhodné nastavit veškeré nepoužívané piny do stavu vypnuto nebo analog aby nedocházelo k elektrickým svodům a tím pádem se minimalizoval únik proudu.

Událost	**Popis události**	**LLWU**
NFC_Wakeup_IRQ	Detekce NFC tagu	P6
Charging_IRQ	Začátek nabíjení baterie	P7
Battery_Low_IRQ	Nízký stav baterie	P8
Button_1_IRQ	Stisknuto tlačítko 1	P9
Button_2_IRQ	Stisknuto tlačítko 2	P10

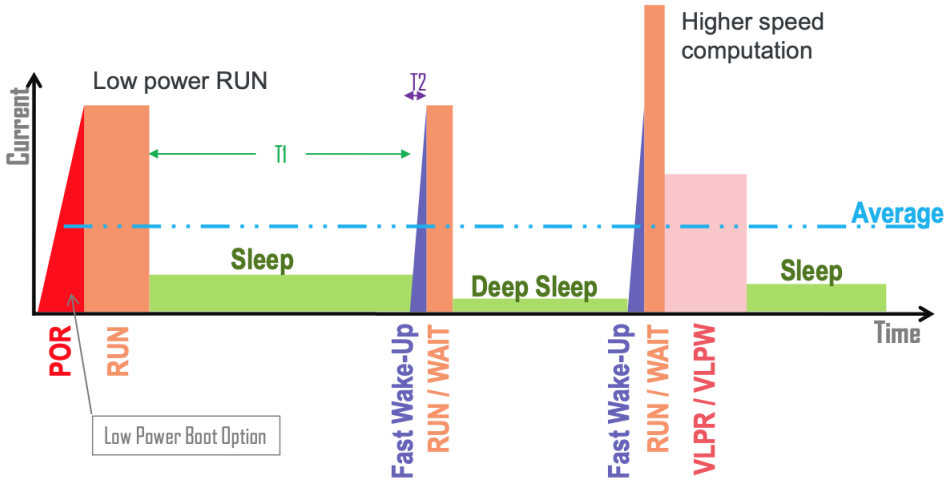
Tab. 3.2: Události pro probuzení mikrokontroléru

Na obrázku 3.2 je znázorněn typický časový průběh běhu aplikace na mikrokontroléru Kinetis.

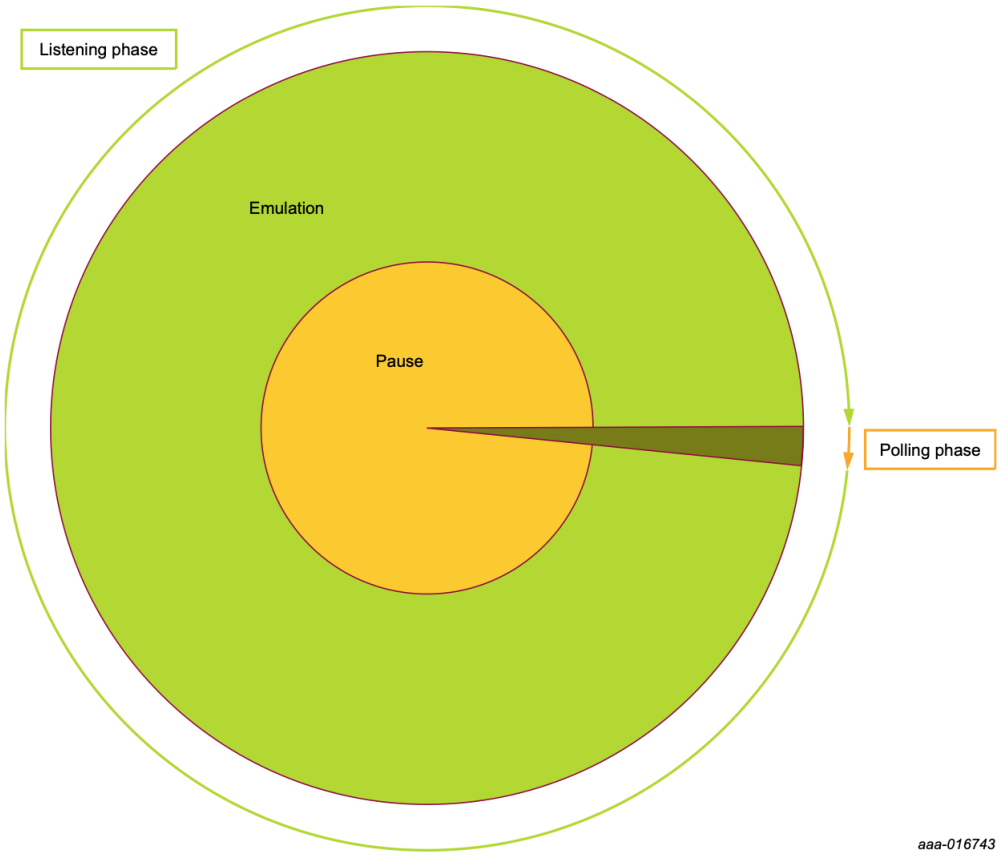
Hlavní událostí pro probuzení představuje detekce tagu NFC, ta je zajišťována čipem PN7150, který má funkci „Low power RF polling“ (3.3), která v nastavených intervalech naslouchá, zda se v blízkosti nenachází NFC tag. Proudový odběr v tomto režimu se pohybuje kolem 150 mikroampérů.

Pokud nastane jedna z událostí pro probuzení, je nejprve vykonána obsluha tohoto přerušení. Pokud se jedná o přerušení NFC Wakeup IRQ, tak se provede autentizace uživatele.

V případě obsluhy přeřušení Charging IRQ se na displeji zobrazí, že baterie je nabíjena. Přerušení Battery Low IRQ značí, že stav baterie je kritický.



Obr. 3.2: Graf spotřeby mikrokontroléru Kinets [26]

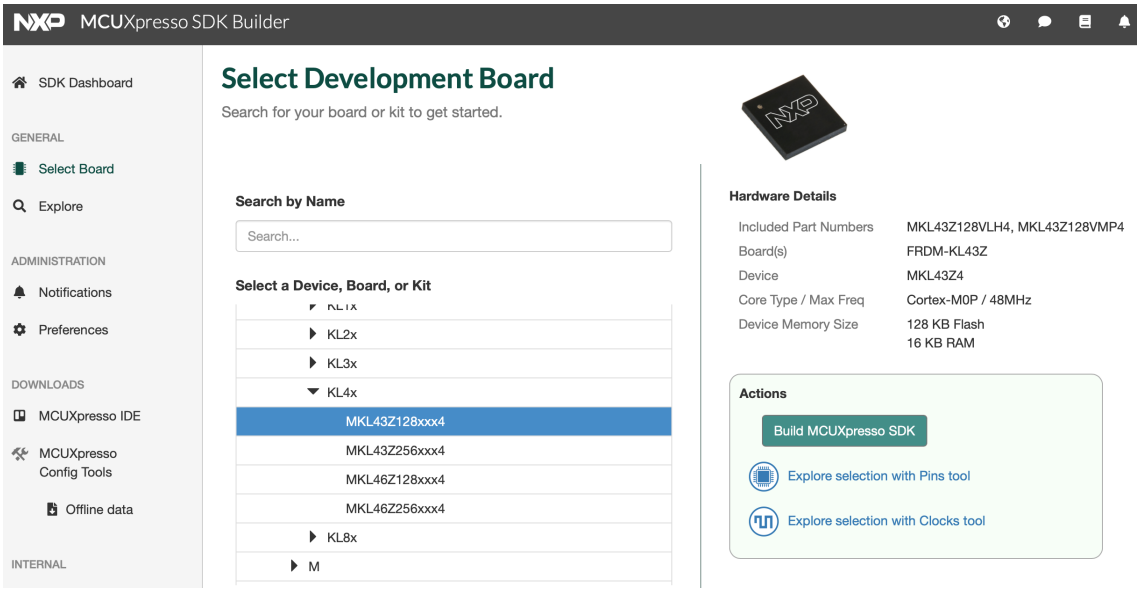


Obr. 3.3: RF low power polling [20]

3.3 Ovladače

K sestavení programu jsou použity ovladače a middleware z MCUXpresso SDK.

Firma NXP dodává k mikrokontrolérům SDK (Software Development Kit) obsahující ovladače k periferiím mikrokontrolérů, jádro systému reálného času FreeRTOS, USB ovladače a také middleware. SDK je dodáváno ve formě archívů ZIP, které je možné vygenerovat na stránkách https://mcuxpresso.nxp.com (3.4), je možné zvolit si potřebné ovladače a middleware a sestavit tak balíček na míru aplikaci. SDK také obsahuje demo aplikace a vygenerovanou dokumentaci.



Obr. 3.4: MCUXpresso SDK Builder [24]

SDK podporuje tři vývojová prostředí – MCUXpresso IDE (jako kompilátor je používán ARM GCC), ARM Keil MDK a IAR Embedded Workbench. Dále je dodáváno vývojové prostředí MCUXpresso IDE a nástroj pro konfiguraci periferií, zdrojů hodinových signálů a nastavení pinů – MCUXpresso Config Tools.

V tabulce 3.3 je seznam potřebných ovladačů pro software chytrého zámku. V tabulce 3.4 je seznam middlewaru, který je nutné přidat do SDK balíčku již při generaci.

Ovladač	Popis	Autor
fsl_common	Podpůrné funkce pro SDK	NXP
fsl_clock	Přepínání hodinových signálů	NXP
fsl_pmc	Power management controller	NXP
fsl_smc	System management controller	NXP
fsl_i2c	Ovladač periferie I2C	NXP
fsl_spi	Ovladače periferie SPI	NXP
fsl_llwu	Ovladač periferie LLWU	NXP
fsl_lptmr	Ovladač nízkopříkonového časovače	NXP
fsl_dmamux	Ovladač DMA multiplexeru	NXP
fsl_gpio	Ovladač GPIO periferie	NXP
fsl_port	Ovladač portů	NXP
fsl_tpm	Ovladač časovače pro generování PWM	NXP
fsl_rcm	Ovladač pro reset control modul	NXP
fsl_flash	Ovladač pro flash modul	NXP
fsl_ftfx	Ovladač pro flash modul	NXP
epaper_2in13	Ovladač displeje	Waveshare, Marek Vitula
ltc2942	Ovladač pro modul LTC2941-2	LonelyWolf, Marek Vitula

Tab. 3.3: Seznam použitých ovladačů

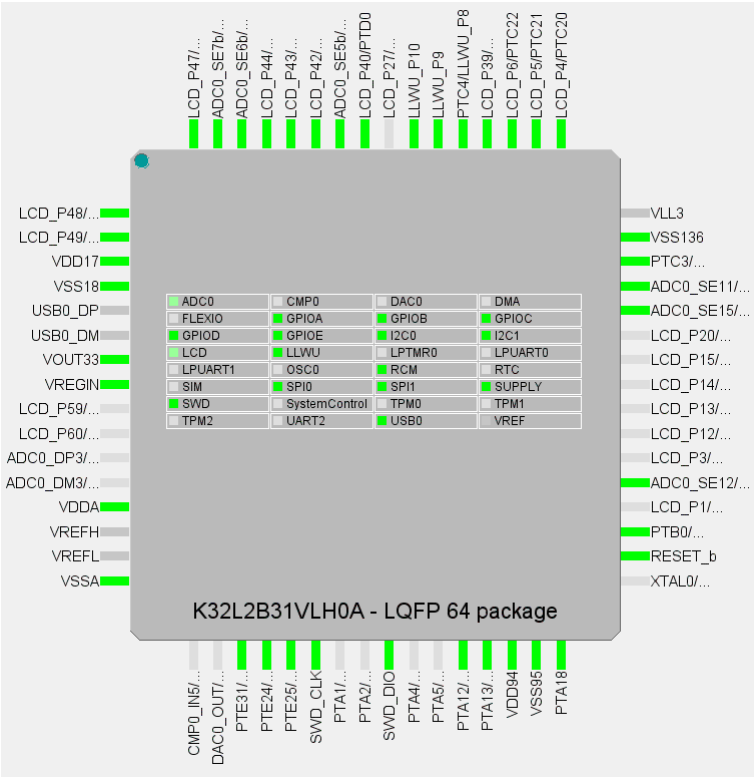
Middleware	Popis	Autor
Sigfox	Ovladač pro OL2385 postavený na vrstvě AML	NXP
AML	Analog middleware layer	NXP
TML	Vrstva middleware pro NFC Library	NXP
NFC library	Knihovna pro práci s NFC	NXP
Fonts	Knihovna fontu pro displej	STMicro
GUI Library	Grafická knihovna pro displej	Waveshare

Tab. 3.4: Seznam použitého middleware

3.4 Konfigurace pinů

Piny na mikrokontroléru Kinetis je možné multiplexovat a lze nastavit až 8 alternativních funkcí. Pro konfiguraci lze využít nástroje NXP Config Tools, který mimo nastavení výstupu pinů umožňuje nastavovat také periferie a zdroje hodinových signálů.

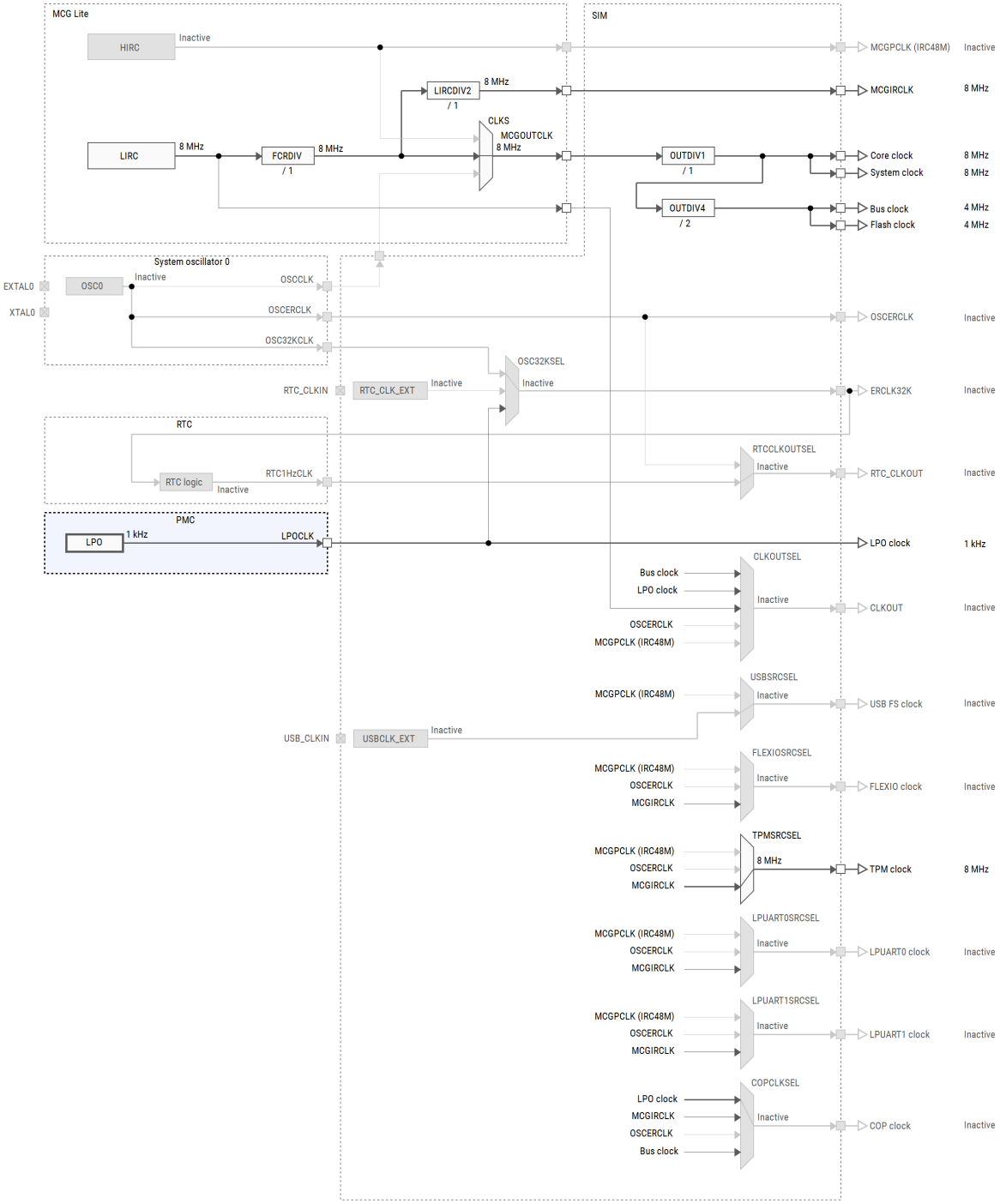
Na obrázku 3.5 je konfigurace pinů pro mikrokontrolér K32L2B použitý pro chytrý zámek. Výstupem takové konfigurace je soubor pin_mux.c, který nakonfiguruje potřebné registry pro multiplexování pinů.



Obr. 3.5: Nastavení pinů pro K32L2B

3.5 Konfigurace hodinových signálů

Na obrázku 3.6 je konfigurace hodinových signálů mikrokontroléru pro režim RUN. Z obrázku je patrné, že je použit oscilátor LIRC 8 MHz jako systémový. Z tohoto oscilátoru je taktována hlavní sběrnice a flash kontrolér. Pro jednotku LLWU je využit nízkopříkonový oscilátor LPO 1 kHz. Pro vygenerování inicializačního kódu bylo využito nástroje NXP Config Tools.



Obr. 3.6: Nastavení hodin pro K32L2B

3.6 NFC

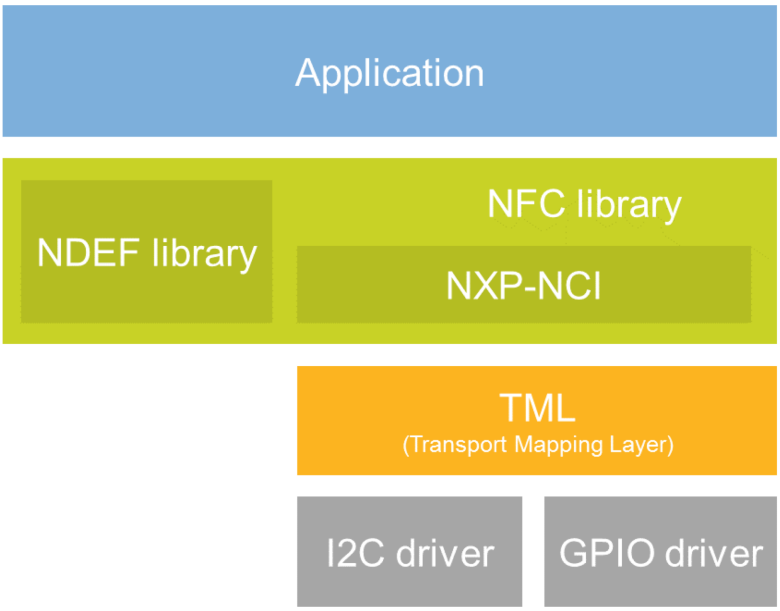
3.6.1 NFC Library

NFC Library je knihovna pro práci s NFC technologií napsaná v jazyce C. Podporuje režimy R/W – čtení a zápis NDEF záznamu z NFC forum zařízení typu 2 nebo typu 4 a autentizace Mifare Classic. Dále podporuje čtení tagů standardu ISO14443-3A, ISO14443-4 a tagů ISO15693. Dalším podporovaným režimem je P2P (Peer-to-Peer) – tedy přímá výměna NDEF záznamů mezi jednotlivými zařízeními. Posledním podporovaným režimem je emulace karty.

NFC Library se skládá ze dvou modulů NXP-NCI a NDEF library. NXP-NCI je vysokoúrovňové API jenž umožňuje konfigurovat NFC kontrolér a spouštět a kontrolovat proces hledání NFC tagů. NDEF library se skládá ze tří submodulů RW_NDEF, P2P_NDEF a T4T_NDEF_emu, které definují již zmíněné tři podporované režimy. TML modul se stará a hardwarovou abstrakci volání I2C a GPIO ovladačů.

Knihovna v plné konfiguraci (s podporou veškerých režimů) zabírá zhruba 8000 bajtů na zásobníku (kompilované pro Cortex-M0 v release konfiguraci), avšak paměťovou náročnost je možné snížit definováním pouze potřebných režimů.

Na obrázku 3.7 je vyobrazena architektura knihovny NFC Library.



Obr. 3.7: Architektura NFC knihovny [33]

3.6.2 Autentizace uživatele

Autentizace uživatele probíhá v několika fázích. První fáze je ověření UID z databáze povolených UID, které jsou uloženy ve struktuře User,

Druhá fáze je autentizace sektoru 1 tajným klíčem. Následuje přečtení tajného klíče pro autentizaci uživatele, který je uložený pouze pro čtení v bloku 4.

Pokud je klíč povolený, tak dojde k autorizaci uživatele. Na následujících řádcích je ukázka autentizace a čtení paměti tagu Mifare Classic s pomocí knihovny NFC Library.

```
/* číslo paměťového bloku */
#define BLK_NB_MFC      4
/* 48bitový klíč pro autentizaci Mifare Classic */
#define KEY_MFC         0x2F, 0x12, 0xAC, 0xA8, 0x54, 0xD4

status_t status = 0;
unsigned char Resp[256];
unsigned char RespSize;
/* Příkaz autentizace sektoru 1 klíčem */
unsigned char Auth[] = {0x40, BLK_NB_MFC/4, 0x10, KEY_MFC};
/* Příkaz čtení bloku 4 */
unsigned char Read[] = {0x10, 0x30, BLK_NB_MFC};
/* Autentizace */
status |= NxpNci_ReaderTagCmd(Auth, sizeof(Auth), Resp, &RespSize);
/* čtení */
status |= NxpNci_ReaderTagCmd(Read, sizeof(Read), Resp, &RespSize);
```

3.7 Sigfox

3.7.1 Ovladač

Ovladač pro OL2385 a OL2361 postavený na vrstvě AML (Analog middleware layer). AML je vrstva kompatibility mezi nízkoúrovňovými ovladači. Je možné využít jak Kinetis SDK 2.0, tak S32 SDK.

Ovladač se skládá z modulu pro nastavení sf_setup, modulu sf_ol23xx, který definuje jednotlivé SPI rámce pro komunikaci se zařízením OL2385. Modul sf implementuje hlavní funkcionalitu.

Hlavní konfigurace Sigfox je ve struktuře sf_user_config_t.

```
typedef struct
{
    sf_net_standard_t netStandard; //  Standard komunikace
    uint8_t txAttSteps;            // Atenuátor po 0,25 dB krocích
    sf_xtal_type_t xtal;           // typ oscilátoru
    sf_tx_repeat_t txRepeat;       // Kolikrát se má opakovat odesílání
    sf_pa_type_t paType;           // Zesílení 0 nebo 14 dBm
} sf_user_config_t;
```

3.7.2 Struktura zprávy

Limit velikosti zprávy (payload) v uplinku je 12 bajtů. Delší zpráva znamená delší dobu odesílání. Pro rádiovou konfiguraci RC1 je doba odesílání zprávy o velikosti 12 bajtů 2 sekundy. Prázdná zpráva se odesílá 1,1 sekundy. Kratší zpráva má tedy za výsledek nižší spotřebu zařízení.

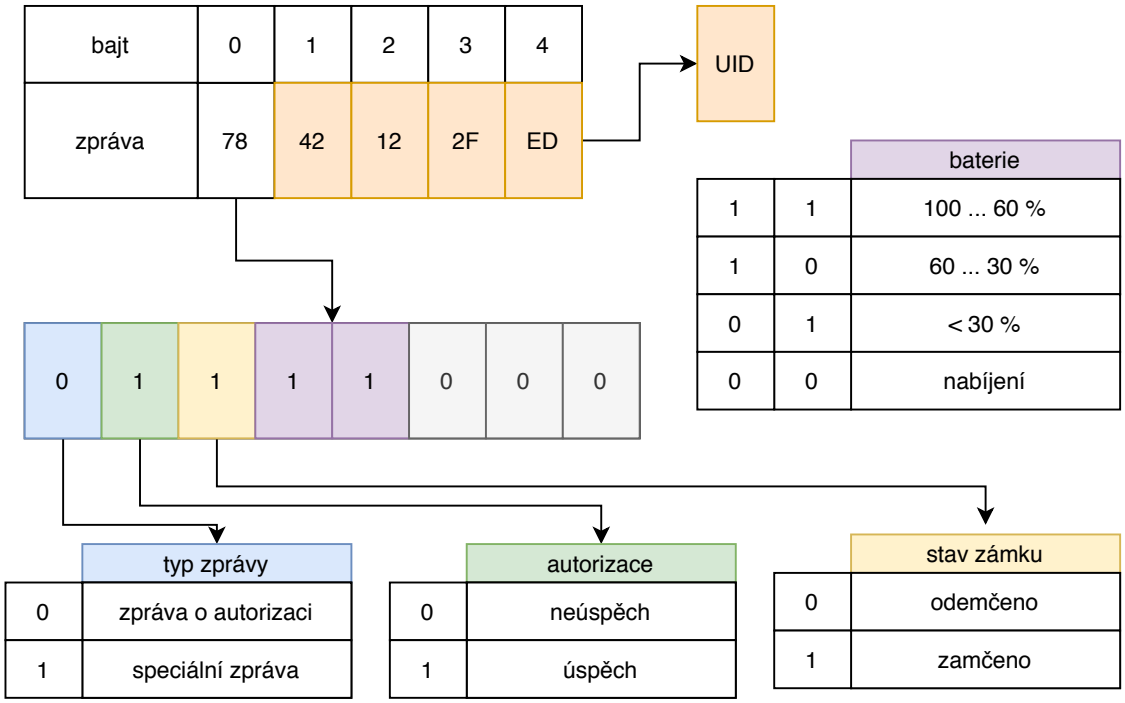
Obsahem zprávy, která je odeslána po autorizování NFC tagu je UID NFC tagu, informace o tom zda došlo k otevření či uzamčení zámku a stav baterie. Struktura zprávy je vyobrazena na obr. 3.8.

3.7.3 Backend

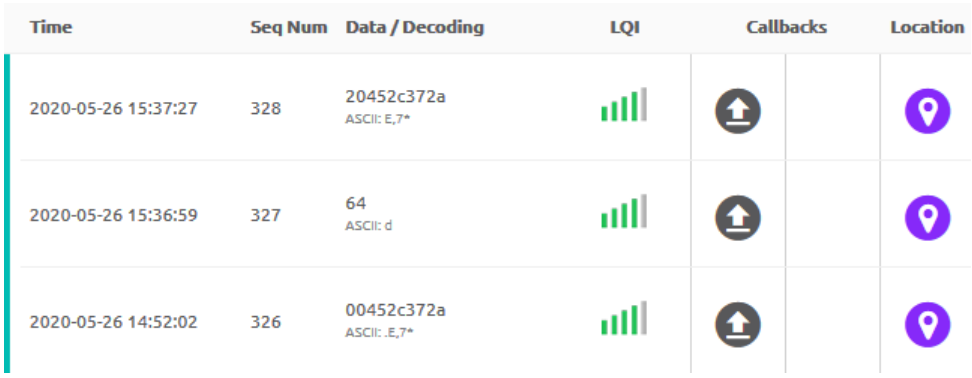
Sigfox backend je webové rozhraní umožňující správu registrovaných Sigfox zařízení. Jsou zde také k dispozici statistiky přenosu a odeslané zprávy. Na odeslané zprávy je možné reagovat pomocí callback funkcí, které lze definovat přes aplikační rozhraní.

Sigfox backend také poskytuje aplikační rozhraní (API) pro automatizovanou správu zařízení. Aplikační rozhraní existuje ve dvou verzích V1 a V2, přičemž verze V1 je zastaralá a podpora je ukončena ke konci března 2020.

Na obrázku 3.9 jsou vypsány přijaté zprávy z chytrého zámku. S těmito daty je pak možné dál pracovat.



Obr. 3.8: Struktura Sigfox zprávy



Obr. 3.9: Přijaté zprávy zobrazené v Sigfox Backend

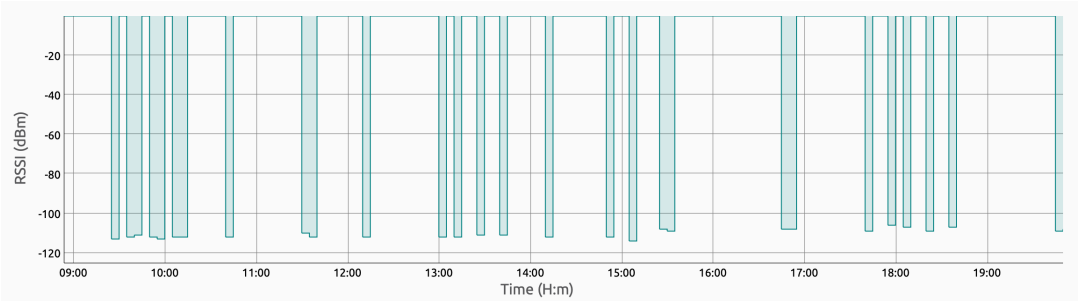
3.7.4 Měření spoje

O měření kvality spoje v uplinku se starají základnové stanice (base stations). Informace, které jsou možné přečíst jsou: RSSI – Received Signal Strength Indicator, tedy výkon přijatého signálu v dBm. Odstup signálu od šumu (SNR) vyjádřený v decibelech. Počet základnových stanic, které přijali vyslanou zprávu. Na základě těchto údajů je vypočítáno číslo LQI (Link quality indicator, viz tabulka 3.5), které je orientačním měřítkem kvality. Na obr. 3.10 a 3.11 je výsledek měření RSSI a SNR během dne 1. dubna 2020 v lokalitě Královo Pole. Během dne bylo z chytrého

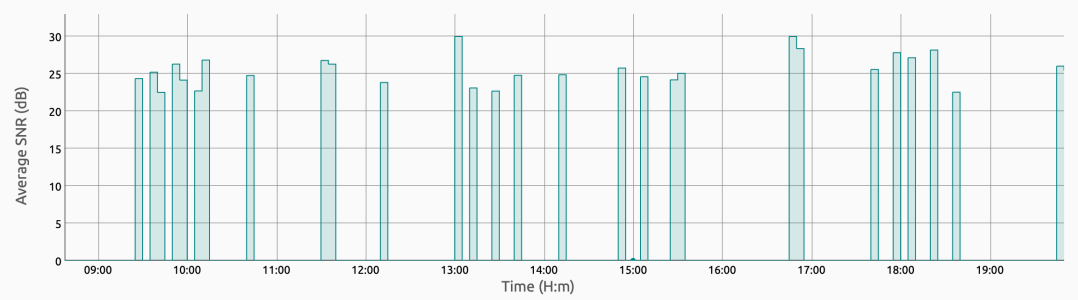
zámku vysláno 30 zpráv s délkou od 2 do 12 bajtů. Maximální naměřená hodnota RSSI byla -107 dBm. Kvalita podle metriky LQI byla u všech zpráv vyhodnocena jako excellent. Průměrná hodnota odstupu signálu od šumu byla 25,4 dB.

RSSI	**Základnové stanice**	**LQI**
-122 dBm <RSSI	3	EXCELLENT
-135 dBm <RSSI $\leq$ -122 dBm	3	GOOD
-122 dBm <RSSI	1 nebo 2	GOOD
-135 dBm <RSSI $\leq$ -122 dBm	1 nebo 2	AVERAGE
RSSI $\leq$ -135 dBm	jakýkoliv počet	LIMIT

Tab. 3.5: Kvalita spoje v síti Sigfox



Obr. 3.10: Měření RSSI během dne v lokalitě Královo Pole



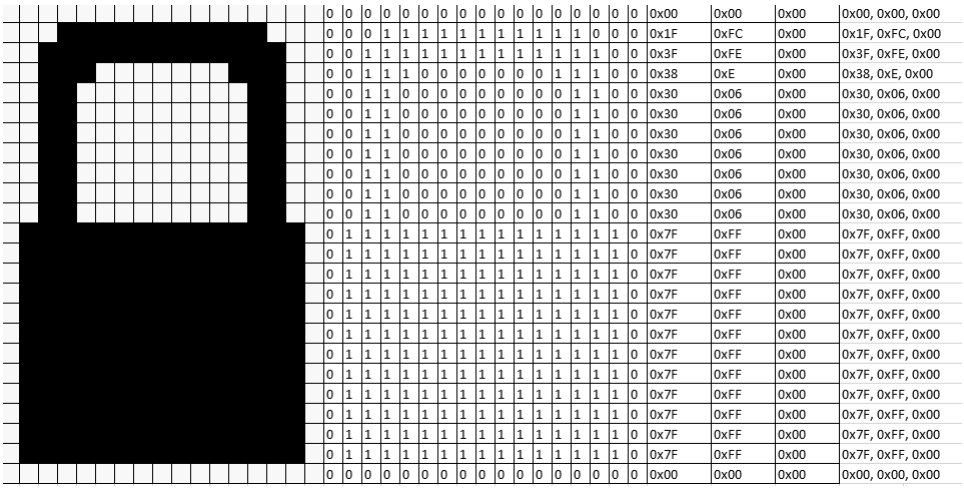
Obr. 3.11: Měření SNR během dne v lokalitě Královo Pole

3.8 Displej

Ovladač displeje byl naportován z verze pro mikrokontrolér STM32 využívající HAL vrstvu na Kinetis SDK verze 2. Zdrojové kódy verze pro STM32 je možné stáhnout z git repozitáře: https://github.com/waveshare/e-Paper.

Displej podporuje režimy částečného překreslení a plného překreslení. Částečné překreslení ale zanechává na displeji artefakty. Pro chytrý zámek byl tedy použit režim plného překreslení.

Součástí ovladače je knihovna s fontem ve velikostech 8, 16, 20 a 24 pixelů. Některé méně používané znaky z knihovny 24 pixelového fontu byly přemapovány pro užitečné symboly jako například ukazatel stavu baterie, ikony NFC a Sigfox a ikona zámku. Na obrázku 3.12 je ukázka z Excel aplikace pro návrh symbolů fontu, která vznikla v rámci řešení diplomové práce.



0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0x00	0x00	0x00, 0x00, 0x00
0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0x1F	0xFC	0x00, 0x1F, 0xFC, 0x00
0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0x3F	0xFE	0x00, 0x3F, 0xFE, 0x00
0	0	1	1	1	0	0	0	0	0	0	0	1	1	1	0	0	0	0x38	0xE	0x00, 0x38, 0xE, 0x00
0	0	1	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0x30	0x06	0x00, 0x30, 0x06, 0x00
0	0	1	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0x30	0x06	0x00, 0x30, 0x06, 0x00
0	0	1	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0x30	0x06	0x00, 0x30, 0x06, 0x00
0	0	1	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0x30	0x06	0x00, 0x30, 0x06, 0x00
0	0	1	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0x30	0x06	0x00, 0x30, 0x06, 0x00
0	0	1	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0x30	0x06	0x00, 0x30, 0x06, 0x00
0	0	1	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0x30	0x06	0x00, 0x30, 0x06, 0x00
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0x7F	0xFF	0x00, 0x7F, 0xFF, 0x00
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0x7F	0xFF	0x00, 0x7F, 0xFF, 0x00
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0x7F	0xFF	0x00, 0x7F, 0xFF, 0x00
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0x7F	0xFF	0x00, 0x7F, 0xFF, 0x00
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0x7F	0xFF	0x00, 0x7F, 0xFF, 0x00
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0x7F	0xFF	0x00, 0x7F, 0xFF, 0x00
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0x7F	0xFF	0x00, 0x7F, 0xFF, 0x00
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0x7F	0xFF	0x00, 0x7F, 0xFF, 0x00
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0x7F	0xFF	0x00, 0x7F, 0xFF, 0x00
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0x7F	0xFF	0x00, 0x7F, 0xFF, 0x00
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0x7F	0xFF	0x00, 0x7F, 0xFF, 0x00
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0x7F	0xFF	0x00, 0x7F, 0xFF, 0x00
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0x00	0x00	0x00, 0x00, 0x00

Obr. 3.12: Tvorba symbolu pro displej

Displej rovněž umožňuje zobrazovat obrázky a grafiku. K tomuto účelu slouží knihovna GUI_Paint. K převodu obrázku do formátu vhodného pro displej je možné využít například nástroje ImageToEpaperConverter

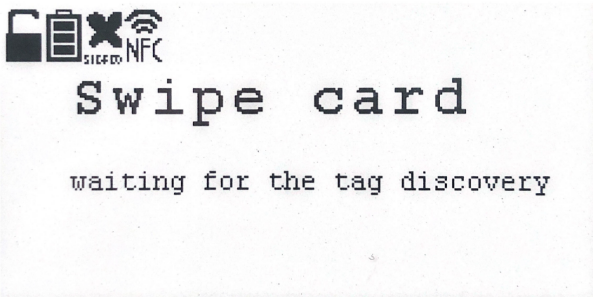
https://github.com/Wh1teRabbitHU/ImageToEpaperConverter. Před použitím je ale nutné obrázek zrcadlit kvůli specifickému adresování v druhé verzi displeje.

Pro pohodlnější řízení displeje byl vytvořen modul display.c, který obsahuje strukturu lockStatus. Tato struktura obsahuje informace o stavu zámku a dále také informace o tom zda byla inicializována komunikace se sítí Sigfox, zda běží NFC a stav baterie.

```
typedef struct {
        bool locked;
        bool sigfoxInit;
        bool NFCInit;
        bool charging;
        int8_t battery;
} LockStatus;
```

Pro zobrazení textu je možné zavolat funkci displayText, jejíž argumenty jsou ukazatele na char main_text, který je na prvním řádku a je vykreslen fontem velikosti 24 a argument second_text, který je vykreslen fontem velikosti 12 na dalším řádku. Zároveň jsou vykresleny i symboly stavu. Na obr. 3.13 a 3.14 je ukázka zobrazení na e-paper displeji.

Obr. 3.13: Zobrazení loga NXP při inicializaci



Obr. 3.14: Zobrazení stavových symbolů

3.9 Řízení obvodu LTC2941

Ovladač obvodu LTC2941 byl naportován z verze pro STM32 od LonelyWolf.

LTC2941 komunikuje po sběrnici I2C/SMB, sedmi bitová adresa zařízení – 1100100 je neměnná. Čip disponuje rovněž pinem pro upozornění na nízké napětí na akumulátoru a také je možné nastavit varování na překročení nastaveného prahu náboje.

3.10 Databáze NFC tagů

Databáze NFC tagů obsahuje informace o kartách uživatelů, kteří jsou oprávněni otevřít zámek. Tyto informace jsou UID – unikátní identifikátor tagu, 4bajtový nebo 7bajtový. UID rovněž slouží jako identifikátor uživatele zasílaný v Sigfox zprávě. Dále je v databázi uložen klíč pro Mifare autorizaci a autorizační klíč (heslo) uložený v NFC tagu. Toto heslo je 16bajtové a je předem náhodně vygenerované. První pozice v databázi náleží tzv. master tagu. Tento tag nelze z databáze vymazat a slouží pro přidávání ostatních tagů do databáze.

```
typedef struct {
        unsigned char mifareKey[MIFARE_SIZE];
        unsigned char authKey[KEY_SIZE];
        unsigned char uid[UID_SIZE];
} user_t;

static user_t arr_user[USERS];
```

Databáze se ukládá do nevolatilní paměti flash v mikrokontroléru. O zápis se stará jednotka FMC (Flash module controller), která rovněž slouží jako rozhraní mezi systémovou sběrnicí a sběrnicí flash. Databáze se ukládá do posledního sektoru v paměti flash. Mikrokontrolér K32L2B disponuje 256 kB paměti flash o velikosti sektoru 1024 B. Velikost databáze je tedy omezena na 32 uživatelů, tak aby její velikost byla maximálně jeden sektor.

Zapsané bity jsou v paměti flash reprezentovány jako „0“ a smazané bity potom jako „1“. Operace programování mění stav bitu z 1 na 0, ale ne obráceně. Pouze operace mazání mění bit z 0 na 1. Před programováním paměti flash je tedy nutné paměť nejprve vymazat. Programování flash paměti se provádí voláním SDK funkce *FLASH_Program*.

```
FLASH_Program(&s_flashDriver, destAdrss,
(uint8_t *)&arr_user, sizeof(arr_user));
```

3.11 Zdrojové kódy

Zdrojový kód firmware byl uvolněn pod licencí 3-Clause BSD. Je možné ho stáhnout z git repozitáře https://github.com/marekvi95/smartlock-fw Návrh hardware byl uvolněn pod stejnou licencí a je možné ho stáhnout z repozitáře

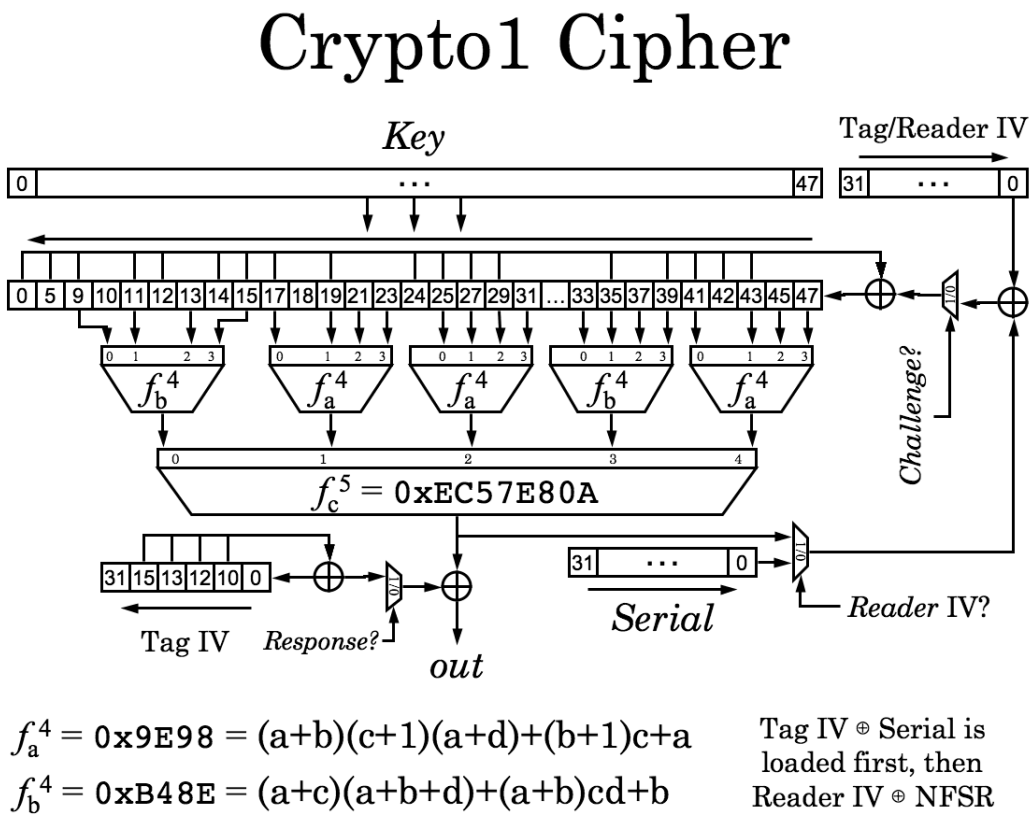
https://github.com/marekvi95/smartlock-hw.

4 Zabezpečení

Cílem této práce je navrhnout zámek ovládaný pomocí technologie NFC. Je tedy vhodné diskutovat samotnou bezpečnost takového řešení po stránce elektronické. Vynechme tedy mechanickou odolnost zámku a cylindrické vložky.

Technologie NFC je v dnešní době velmi rozšířená a to i v oblastech, které jsou velmi citlivé na bezpečnost jako je například řízení přístupu v budovách, platební systémy, doprava, atd. Karty ISIC používáné na VUT jsou rovněž standardu Mifare Classic.

Jeden z nejpoužívanějších systémů v NFC je Mifare Classic. Tento systémy používá proprietární 48bitovou šifru CRYPTO-1, která byla publikována v roce 2008 společností NXP (v té době Philips). Šifra byla prolomena v roce 2009. Na obrázku 4.1 je znázorněna funkce šifry.



Obr. 4.1: Šifra Crypto-1 (blackhat.com)

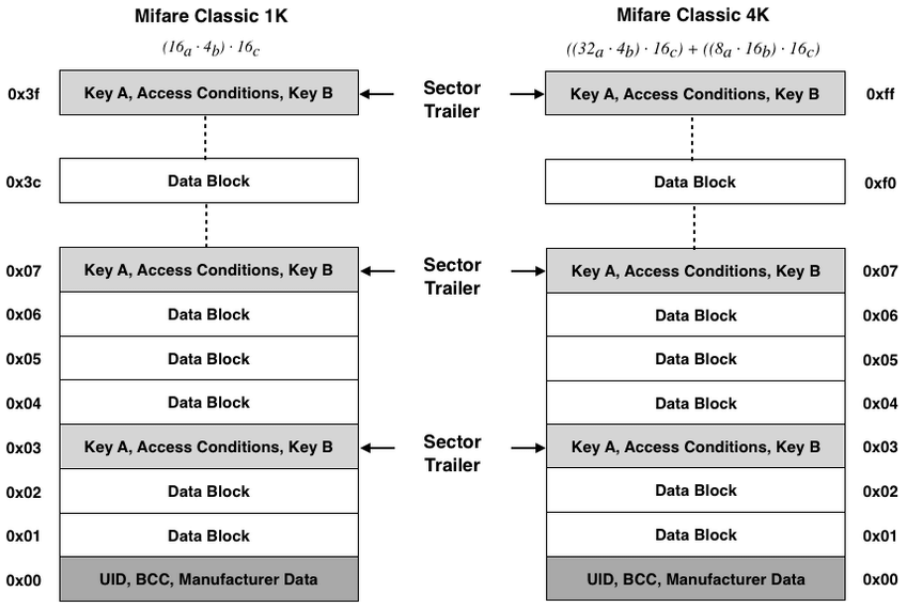
Šifra obsahuje pro účely autentizace posuvný registr s lineární zpětnou vazbou, který slouží jako generátor pseudonáhodných čísel určený polynomem.

$$x^{16} + x^{14} + x^{13} + x^{11} + 1$$

U tohoto registru je využíváno pouze 16 bitů, ačkoliv je 32bitový. Generuje tedy pouze 65536 čísel, což při běžné komunikační rychlosti dojde k opakování sekvence každou 0,6 sekundy.

Na obrázku 4.2 je schéma paměti na kartách Mifare Classic 1k a 4k. Blok 0 obsahuje výrobní data a identifikátor karty UID, který je buď čtyř nebo sedmi bajtový. Tento je dle specifikace Mifare[21] pouze pro čtení, ale je možné zakoupit čínské padělky u kterých je možné zapisovat do bloku 0. Na tomto místě je nutné zmínit stav zabezpečení karet využívaných na VUT, kde je k autentizaci vyžadováno pouze UID karty.

Každý sektor obsahuje jeden blok tzv. sector trailer, kde se nachází klíč A a B a také registr AC, který nastavuje práva k přístupu k jednotlivým blokům.



Obr. 4.2: Schéma paměti Mifare [21]

Dalším problémem je dle společnosti Nethemba časté využívání výchozích klíčů pro šifrování jako např. 0xffffffffffff.

Problémem samotného šifrování CRYPTO-1 je i to, že je pouze 48bitová, což je na moderních FPGA prolomitelné metodou brute force v řádu hodin. Dalším problémem je už zmíněný posuvný registr s lineární zpětnou vaznou, který je deterministický. Na této zranitelnosti jsou postavené další útoky, zmiňme například Nested attack, který byl publikován Nijmegan Oaklandem v roce 2009. Tento útok byl implementován v podobě nástroje MFOC.

Klonování karty je poměrně jednoduché, pokud jsme získali veškeré klíče, tak je možné provést kopii. Při použití speciálních karet lze zkopírovat i identifikátor UID a získat tak 100% kopii karty.

4.1 Doporučení k technologii Mifare

NXP nedoporučuje používat karty Mifare Classic pro bezpečnostní aplikace. Jako zatím bezpečnou alternativu lze použít karty Mifare Plus a Mifare DESFire EV1 či EV2, které disponují šifrováním AES-128[34].

4.2 Bezpečnost sítě Sigfox

Síť Sigfox je využívána pouze pro odesílání údajů o autentizaci uživatelů, nelze ji tedy přímo zneužít k ovládání dveří. Bezpečnost tedy není natolik klíčová.

K šifrování zpráv (payloadu) Sigfox využívá šifrování AES-128, tato šifra je dnes obecně považována za bezpečnou. Ale byla publikována jiná zranitelnost Sigfox replay attack[37], která zneužívá 12bitové číslo zprávy SN (sequence number). Toto číslo značí pořadí odeslané zprávy, existuje tedy pouze 4096 možností a toho je možné zneužít.

4.3 Bezpečnost použitého mikrokontroléru

Mikrokontrolér K32L2B nedisponuje pokročilými bezpečnostními funkcemi jako je například generátor náhodných čísel nebo akcelerátor šifrování. Jediná funkce bezpečnostní funkce, kterou tento mikrokontrolér disponuje je 80bitové unikátní číslo, které je neměnné.

Při uvedení zařízení do produkce je také vhodné zabezpečit port SWD a rozhraní, které umožňují přistoupit k ROM bootloaderu. Nastavení přístupových práv paměti flash je prováděno v 16bajtovém registru.

5 Závěr

Výstupem celé diplomové práce je technická dokumentace pro výrobu desky plošných spojů pro chytrý zámek včetně obslužného firmwaru pro mikrokontrolér. Chytrý zámek byl rovněž sestaven a byla demonstrována jeho funkčnost na prototypu dveří do kterých byl zámek zabudován. Deska plošných spojů obsahuje modul pro NFC a pro Sigfox. Byla vyzkoušena komunikace s NFC tagy standardu Mifare Classic a také se sítí Sigfox. Nad rámec zadání byla realizována databáze NFC tagů v paměti flash. Zámek umožňuje autentizaci uživatele pomocí NFC tagu a následné odeslání zprávy do sítě Sigfox. Zámek rovněž umožňuje otevřít standardní cylindrickou vložku.

Tagy standardu Mifare Classic je vhodné vyměnit za standard o vyšší bezpečnosti, například Mifare DESFire EV2. Podrobnosti jsou uvedeny v kapitole o bezpečnosti. Pokračování práce by také mohlo být vyřešení webového frontendu pro komunikaci se sítí Sigfox.

Literatura

[1] Gartner *Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020* [online]. 2019 [cit. 10. 11. 2019]. Dostupné z URL: <https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io>.

[2] RHODES, BRIAN *Designing Access Control Guide* [online]. 2019 [cit. 10. 11. 2019]. Dostupné z URL: <https://ipvm.com/reports/designing-an-access-control-system>.

[3] Smart Lock Scout *Residential Smart Locks* [online]. 2019 [cit. 10. 11. 2019]. Dostupné z URL: <https://www.postscapes.com/smart-lock-companies/>

[4] Assa Abloy *Chytré otvírání FAB ENTR* [online]. 2019 [cit. 10. 11. 2019]. Dostupné z URL: <https://www.fab.cz/cs/site/fabcz/chytre-otevirani/>

[5] NXP *UM11232 NFC Antenna Design Tool User Guide* [online]. 2019 [cit. 22. 10. 2019]. Dostupné z URL: <https://www.nxp.com/docs/en/user-guide/UM11232.pdf>.

[6] ST: *AN2972 How to design an antenna for dynamic NFC tags* [online]. 2019 [cit. 22. 10. 2019]. Dostupné z URL: <https://www.st.com/content/ccc/resource/technical/document/application_note/bc/ac/13/fe/69/fb/49/8a/CD00232630.pdf/files/CD00232630.pdf/jcr:content/translations/en.CD00232630.pdf>.

[7] NXP *NFC controller PN7150 datasheet* [online]. 2018 [cit. 22. 10. 2019]. Dostupné z URL: <https://www.nxp.com/docs/en/data-sheet/PN7150.pdf>.

[8] Texas Instruments, Milos Acanski *Selecting the right DC/DC converter for maximum battery life* [online]. 2019 [cit. 28. 10. 2019]. Dostupné z URL: <http://www.ti.com/lit/an/slvae14/slvae14.pdf>.

[9] Sigfox *Sigfox connected objects: Radio specifications* [online]. 2019 listopad v1.4 [cit. 3. 10. 2019]. Dostupné z URL: <https://storage.sbg1.cloud.ovh.net/v1/AUTH_669d7dfced0b44518cb186841d7cbd75/prod_medias/build/40599z1k361d4ht/Sigfox%20radio%20specifications%20v1.4%20%20November%202019.pdf>.

[10] Sigfox *Sigfox coverage* [online]. 2019 [cit. 3. 10. 2019]. Dostupné z URL: <https://www.sigfox.com/en/coverage>.

[11] InnoComm *Sigfox module SN10-11* [online]. 2019 [cit. 3. 10. 2019]. Dostupné z URL: <https://www.innocomm.com/product_inner.aspx?num=123>.

[12] NFC Forum *About the technology* [online]. 2019 [cit. 3. 10. 2019]. Dostupné z URL: <https://nfc-forum.org/what-is-nfc/about-the-technology/>.

[13] RAIDA, ZBYNĚK a kol. *Multimediální učebnice: Elektromagnetické vlny Mikrovlnná technika* [online]. [cit. 23. 10. 2019]. Dostupné z URL: <http://www.urel.feec.vutbr.cz/~raida/multimedia/index.php?nav=9-1-A>.

[14] NXP: *OL2385 Industrial RF transceiver* [online]. 2016 [cit. 23. 10. 2019]. Dostupné z URL: <https://www.nxp.com/docs/en/data-sheet/OL2385.pdf>.

[15] Analog Devices: *LTC2941 Battery Gas Gauge with I2C Interface* [online]. 2018 [cit. 23. 10. 2019]. Dostupné z URL: <https://www.analog.com/media/en/technical-documentation/data-sheets/LTC2941.pdf>.

[16] Analog Devices: *ADP5300 High efficiency, ultralow quiescent current step-down regulator* [online]. 2017 [cit. 23. 10. 2019]. Dostupné z URL: <https://www.analog.com/media/en/technical-documentation/data-sheets/ADP5300.pdf>.

[17] Microchip: *MCP73831 Single Cell, Li-Ion/Li-Polymer Charge Management Controller* [online]. 2014 [cit. 29. 10. 2019]. Dostupné z URL: <http://ww1.microchip.com/downloads/en/DeviceDoc/20001984g.pdf>.

[18] NXP: *MPC17531A 700 mA dual H-Bridge motor driver with 3.0 V compatible logic I/O* [online]. 2014 [cit. 29. 10. 2019]. Dostupné z URL: <https://www.nxp.com/docs/en/data-sheet/MPC17531A.pdf>.

[19] NXP: *AN11756 PN7150 Hardware Design Guide* [online]. 2018 [cit. 23. 10. 2019]. Dostupné z URL: <https://www.nxp.com/docs/en/application-note/AN11756.pdf>.

[20] NXP: *AN11755 PN7150 Antenna Design and Matching Guide* [online]. 2018 [cit. 26. 10. 2019]. Dostupné z URL: <https://www.nxp.com/docs/en/application-note/AN11755.pdf>.

[21] NXP: *MIFARE Classic EV1 1K* [online]. 2018 [cit. 26. 10. 2019]. Dostupné z URL: <https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf>.

[22] NXP: *AN10833 MIFARE Type Identification Procedure* [online]. 2016 [cit. 1. 3. 2020]. Dostupné z URL: <https://www.nxp.com/docs/en/application-note/AN10833.pdf>.

[23] NXP: *K32L2B Guide* [online]. 2019 [cit. 26. 10. 2019]. Dostupné z URL: <https://www.nxp.com/docs/en/fact-sheet/K32-L2-FS.pdf>.

[24] NXP: *MCUXpresso SDK Builder* [online]. 2019 [cit. 26. 10. 2019]. Dostupné z URL: <https://mcuxpresso.nxp.com/en/welcome>.

[25] Freescale Semmiconductor Daniel Martinez, César Manzanarez Guadalajara, México *AN4470 Using Low Power modes on Kinetis family* [online]. 01/2018 [cit. 26. 10. 2019]. Dostupné z URL: <https://os.mbed.com/media/uploads/GregC/an4470-using_low-power_modes_with_kinetis_mcus.pdf>.

[26] NXP: *KinetisLow-Power Capabilities in Real Application Cases* [online]. Freescale Technology Forum 2014 [cit. 26. 10. 2019]. Dostupné z URL: <http://cache.freescale.com/files/training/doc/ftf/2014/FTF-SDS-F0168.pdf>.

[27] Panasonic *Panasonic Interactive Short Form Catalog 2018* [online]. 2018 [cit. 10. 11. 2019]. Dostupné z URL: <https://eu.industrial.panasonic.com/sites/default/pidseu/files/downloads/files/panasonic-batteries-short-form-catalog-2018-\for-professionals_interactive_08_11_18.pdf>.

[28] Battery University (Cadex) *Is Lithium-ion the Ideal Battery?* [online]. 2010 [cit. 10. 11. 2019]. Dostupné z URL: <https://batteryuniversity.com/learn/archive/is_lithium_ion_the_ideal_battery>.

[29] Electronics Notes *NFC Tags and Tag Types* [online]. [cit. 15. 2. 2020]. Dostupné z URL:

<https://www.electronics-notes.com/articles/connectivity/nfc-near-field-communication/tags-types.php>.

[30] Molex *Industrial, Scientific and Medical (ISM) Antennas* [online]. 2019 [cit. 25. 11. 2019]. Dostupné z URL: <http://www.literature.molex.com/SQLImages/kelmscott/Molex/PDF_Images/987650-7461.pdf>.

[31] Waveshare Wiki *2.13inch e-Paper HAT* [online]. 2019 [cit. 25. 2. 2020]. Dostupné z URL: <https://www.waveshare.com/wiki/2.13inch_e-Paper_HAT>.

[32] Øyvind Nydal Dahl *What is an H-Bridge?* [online]. 2018 [cit. 10. 3. 2020]. Dostupné z URL: <https://www.build-electronic-circuits.com/h-bridge/>

[33] NXP *AN11990 NXP-NCI MCUXpresso example* [online]. 2018 [cit. 30. 1. 2020]. Dostupné z URL: <https://www.nxp.com/docs/en/application-note/AN11990.pdf>.

[34] NXP *Security Statement on Crypto1 Implementations* [online]. 2015 [cit. 28. 3. 2020]. Dostupné z URL: <https://www.mifare.net/en/products/chip-card-ics/mifare-classic/security-statement-on-crypto1-implementations/>.

[35] Richter Czech *Stavební 5stavíková knoflíková vložka* [online]. [cit. 30. 3. 2020]. Dostupné z URL: <https://www.richterczech.cz/ep-30-35k-ni>.

[36] Bandrinath Kulkarni *NFC Data Exchange Format (NDEF)* [online]. 2017 [cit. 17. 3. 2020]. Dostupné z URL: <https://ibadrinath.blogspot.com/2012/07/nfc-data-exchange-format-ndef.html>.

[37] Coman, Florian & Malarski, Krzysztof & Petersen, Martin & Ruepp, Sarah. *Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT*. 2019 [cit. 27. 3. 2020]. 1-6. 10.1109/GIOTS.2019.8766430.

[38] Sparkfun *ROB-13258 Hobby gear motor* [online]. [cit. 1. 4. 2020]. Dostupné z URL: <https://www.sparkfun.com/products/13258>.

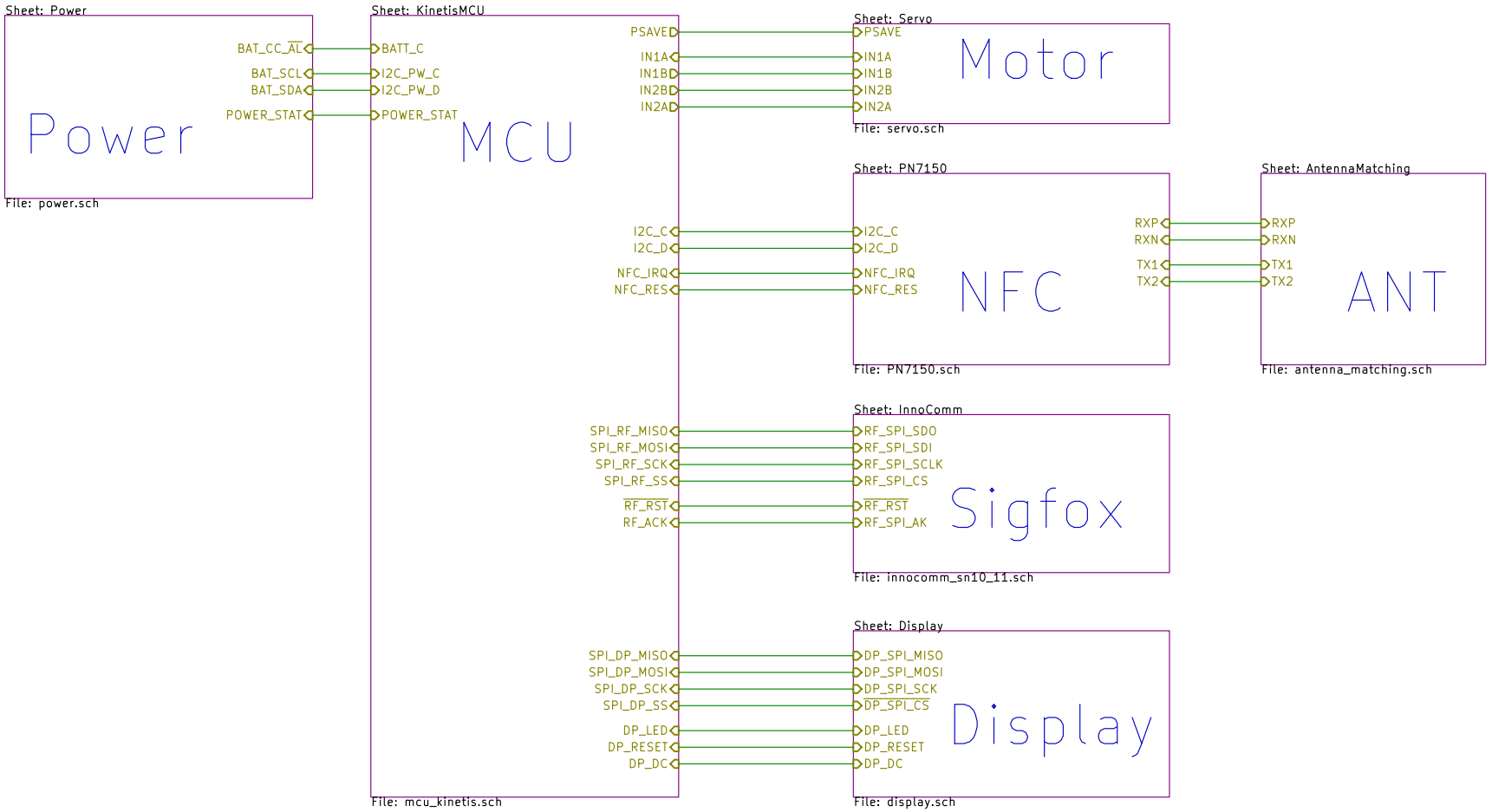
Seznam symbolů, veličin a zkratek

NFC	Modulární technologie radiové bezdrátové komunikace – Near Field Communication
IoT	Internet věcí – Internet of Things
LPWAN	Low-power wide area networks
LoRa	Síť typu LPWAN – Long range
GPS	Globální navigační systém – Global positioning system
DBPSK	Typ digitální modulace – differential BPSK
GFSK	Typ digitální modulace – Gaussian frequency-shift keying
UNB	Velmi úzké pásmo – Ultra narrow band
ETSI	European Telecommunications Standards Institute
EIRP	Efektivní vyzářený výkon – effective radiated power
AES	Standard pokročilého šifrování – Advanced Encryption Standard
CBC	Šifrová zpětná vazba – Cipher block chaining
CRC	Cyklický redundantní součet – Cyclic redundancy check
BCH	Cyklický samoopravný kód – Bose–Chaudhuri–Hocquenghem code
NFC	Near-Field communication
RFID	Identifikace na rádiové frekvenci – Radio Frequency Identification
SPI	Sériové periferní rozhraní – Serial Peripheral Interface
I2C	Multi-masterová počítačová sériová sběrnice – Inter-Integrated Circuit
SDK	Sada vývojových nástrojů – Software development kit
BGA	Typ pouzdra integrovaného obvodu – Ball grid array
RF	Radio frequency
RAM	Polovodičové paměti s přímým přístupem – Random-Access-Memory
RTC	Hodiny reálného času – Real-time clock
LPUART	Low power UART
NVIC	Jednotka pro kontrolu přerušení – Nested Vectored Interrupt Controller
IRQ	Žádost o přerušení – Interrupt ReQuest
ARM	Označení architektury procesorů – Advanced RISC Machine
AWIC	Asynchronous Wakeup Interrupt Controller
SRAM	Statická paměť – Static Random Access Memory
TSI	Touch-Sensing interface
RAM	Pulzně šířková modulace – Pulse Width Modulation
PLL	Fázový závěs – Phase-Locked Loop
TX	Vysílání – Transmit
RX	Příjem – Receive

AGC	Automatické ovládání zisk – Automatic gain control
I/Q	Synfázní a kvadraturní složka – In-phase and quadrature component
RISC	Architektura procesorů – Reduced instruction set computer
EROM	Erasable programmable read-only memory
UHF	Ultra krátké vlny – Ultra high frequency
NRZ	Kódovací technika – non-return-to-zero
HAL	Vrstva abstrakce hardwaru – Hardware abstraction layer
LIN	Sběrnice – Local Interconnect Network
SMA	Koaxiální RF konektor – SubMiniature
SMT	Povrchová montáž – surface mount technology
NCI	NFC Controller Interface
EMC	Elektromagnetická kompatibilita – Electromagnetic compatibility

Seznam příloh

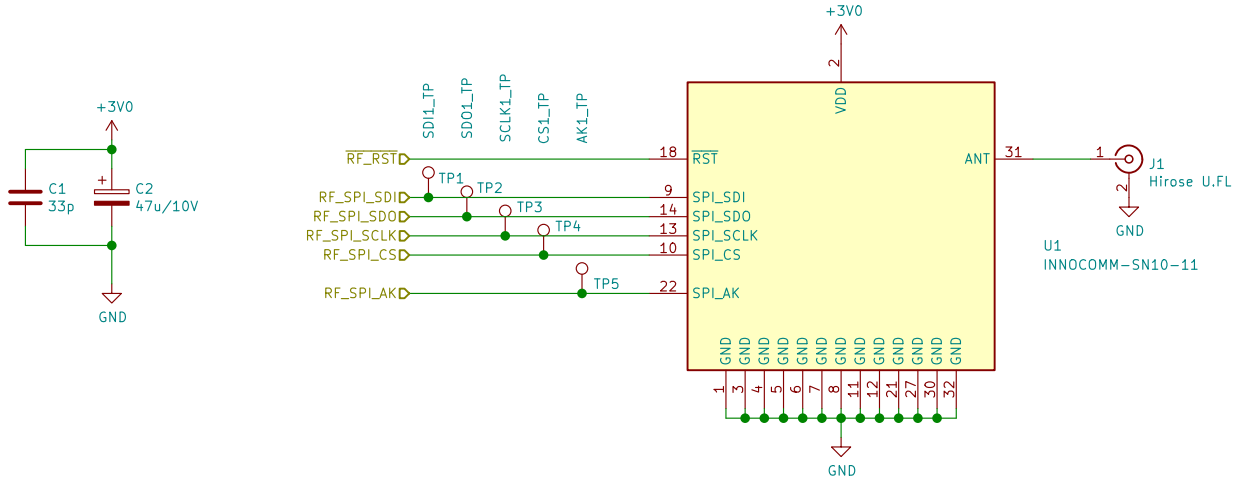
A Elektrické schéma chytrého zámku



Sheet: /
File: smartlock.sch

Title: Smartlock

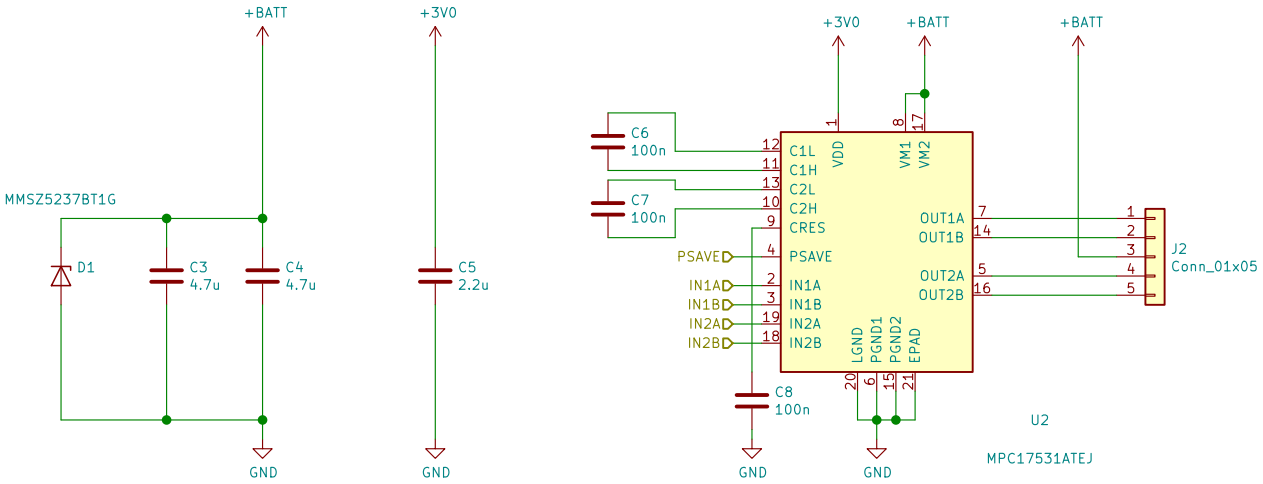
Size: A4	Date: 2019-12-01	**Rev: A0**
KiCad E.D.A. eeschema (5.1.4-0-10_14)		Id: 1/8



Sheet: /InnoComm/
File: innocomm_sn10_11.sch

Title: Sigfox module

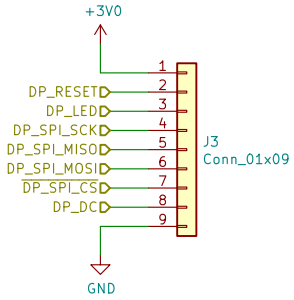
Size: A4	Date: 2019-12-01	**Rev: A0**
KiCad E.D.A. eeschema (5.1.4-0-10_14)		Id: 2/8



Sheet: /Servo/
File: servo.sch

Title: Motor control

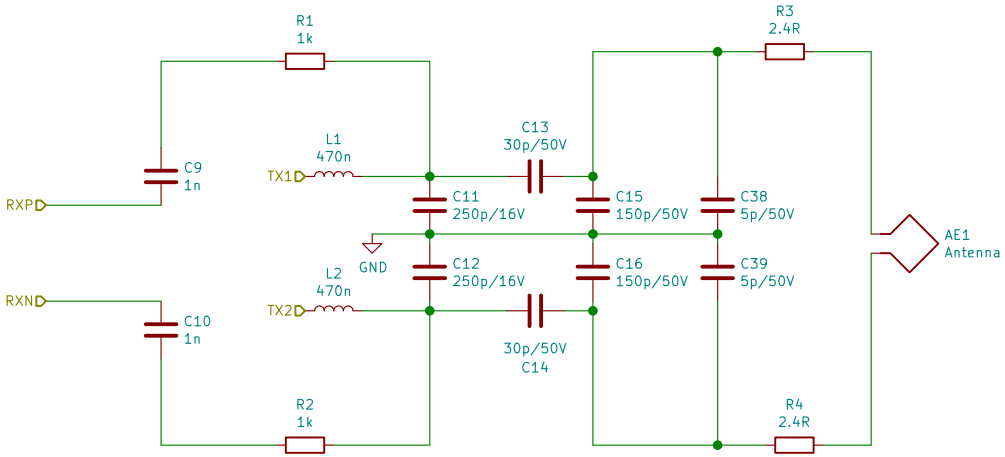
Size: A4	Date: 2019-12-01	**Rev: A0**
KiCad E.D.A. eeschema (5.1.4-0-10_14)		Id: 3/8



Sheet: /Display/
File: display.sch

Title: Display header

Size: A4	Date: 2019-12-01	**Rev: A0**
KiCad E.D.A. eeschema (5.1.4-0-10_14)		Id: 4/8

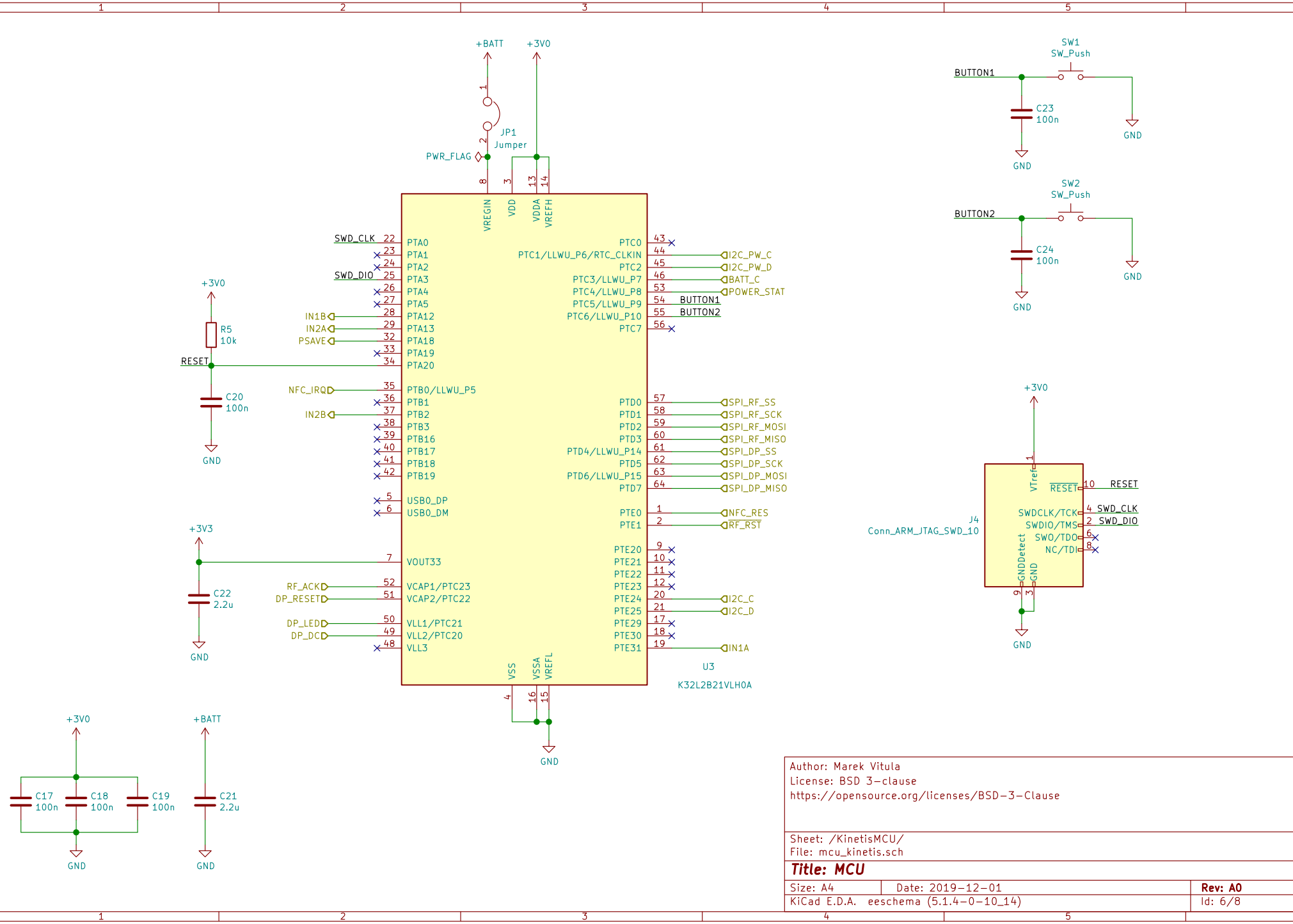


Author: Marek Vitula
License: BSD 3-clause
https://opensource.org/licenses/BSD-3-Clause

Sheet: /AntennaMatching/
File: antenna_matching.sch

Title: Antenna matching

Size: A4	Date: 2019-12-01	**Rev: A0**
KiCad E.D.A. eeschema (5.1.4-0-10_14)		Id: 5/8

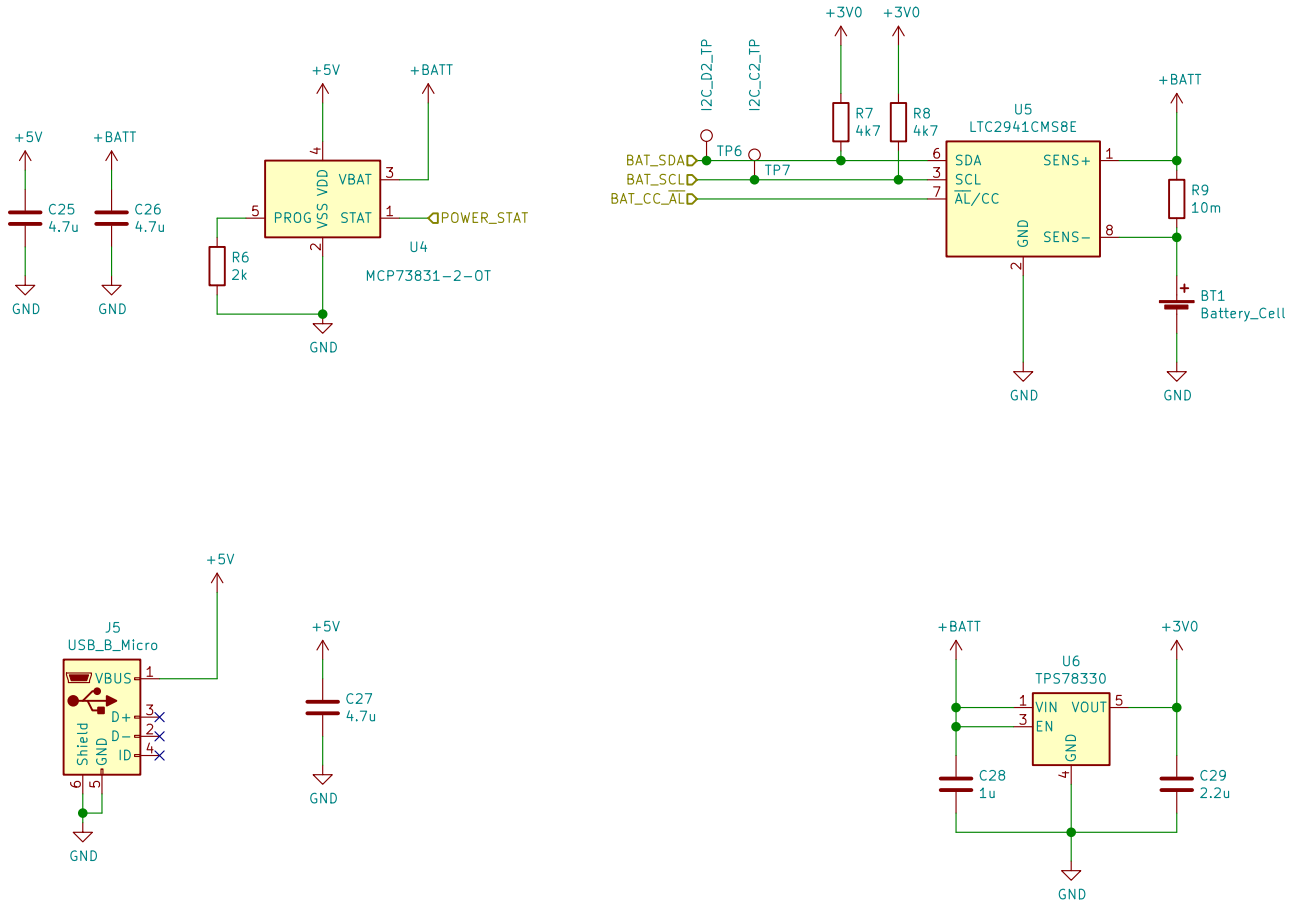


Author: Marek Vitula

Sheet: /KinetisMCU/
File: mcu_kinetis.sch

Title: MCU

Size: A4	Date: 2019-12-01	**Rev: A0**
KiCad E.D.A. eeschema (5.1.4-0-10_14)		Id: 6/8

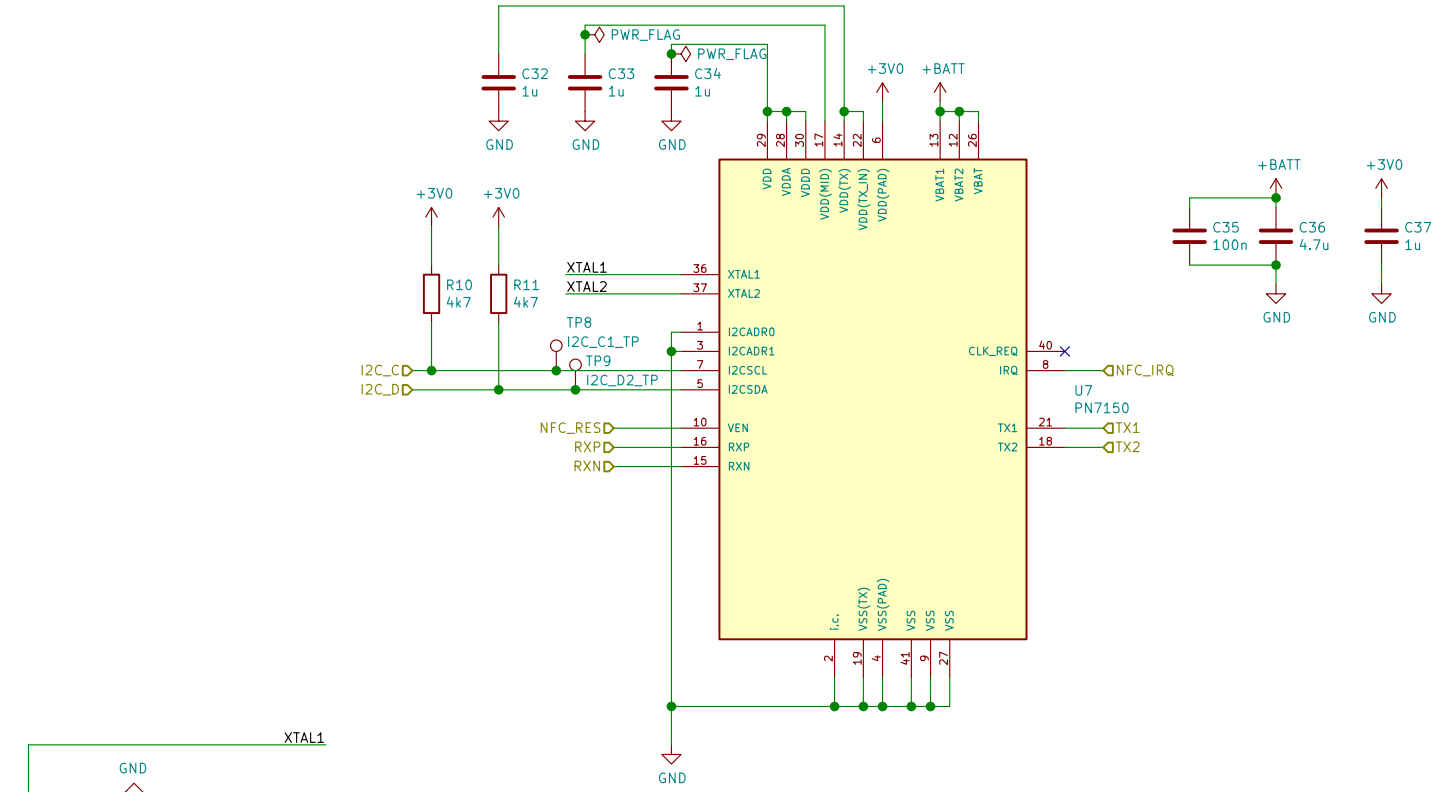


Author: Marek Vitula
License: BSD 3-clause
https://opensource.org/licenses/BSD-3-Clause

Sheet: /Power/
File: power.sch

Title: Power sources, charging and battery monitoring

Size: A4	Date: 2019-12-01	**Rev: A0**
KiCad E.D.A. eeschema (5.1.4-0-10_14)		Id: 7/8



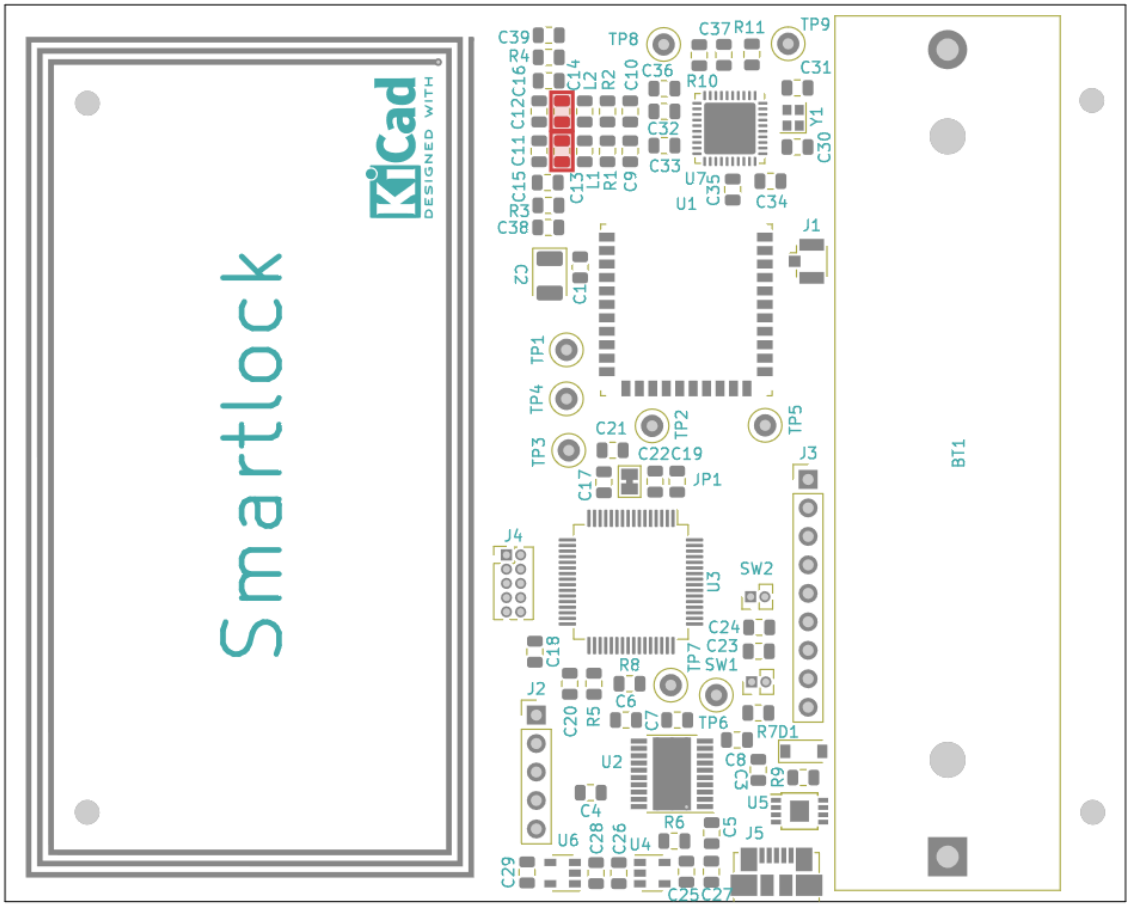
Sheet: /PN7150/
File: PN7150.sch

Title: NFC

Size: A4	Date: 2019-12-01	**Rev: A0**
KiCad E.D.A. eeschema (5.1.4-0-10_14)		Id: 8/8

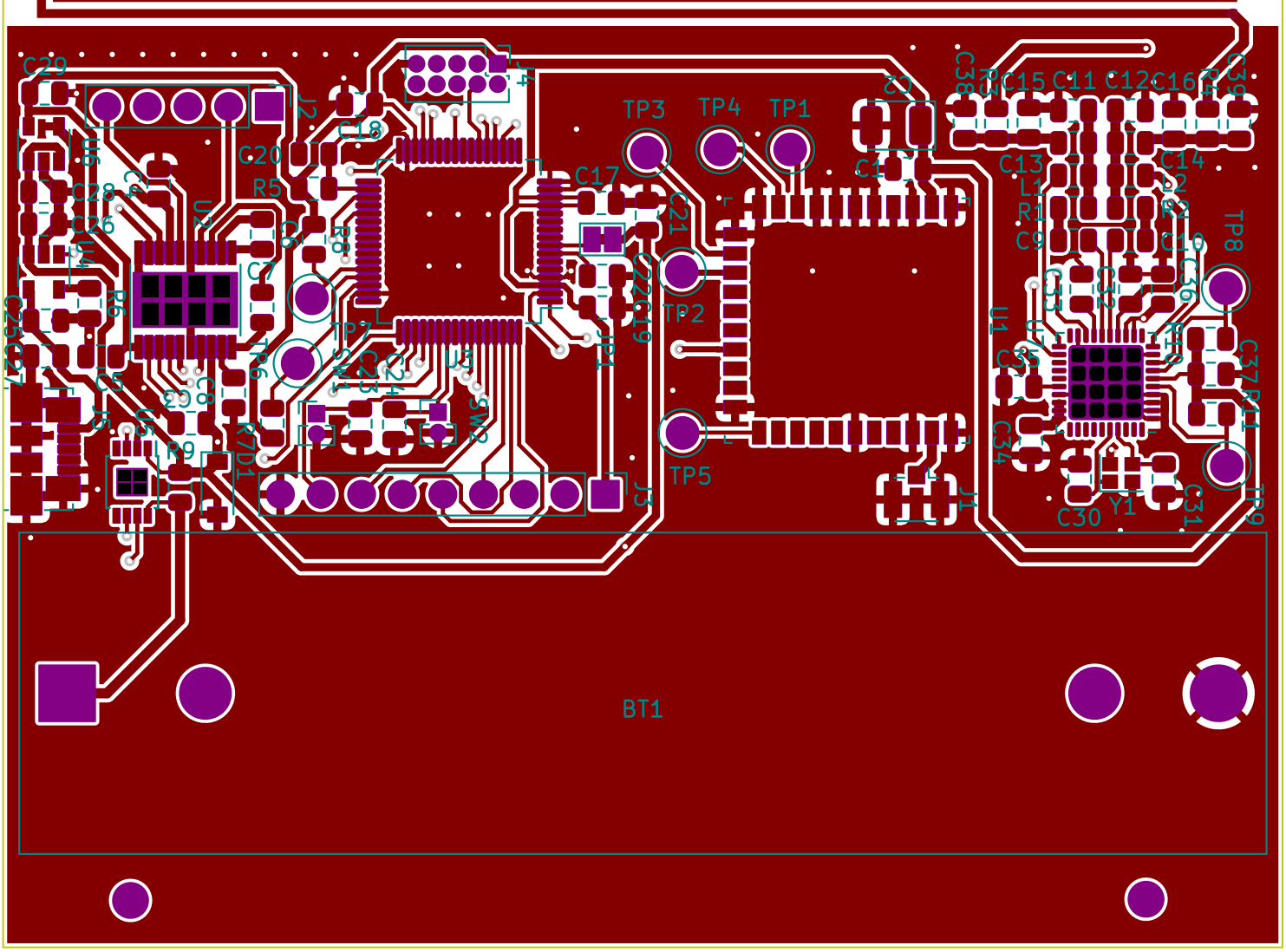
B Výrobní dokumentace

Ná následujících stranách jsou desky plošných spojů exportované do PDF.



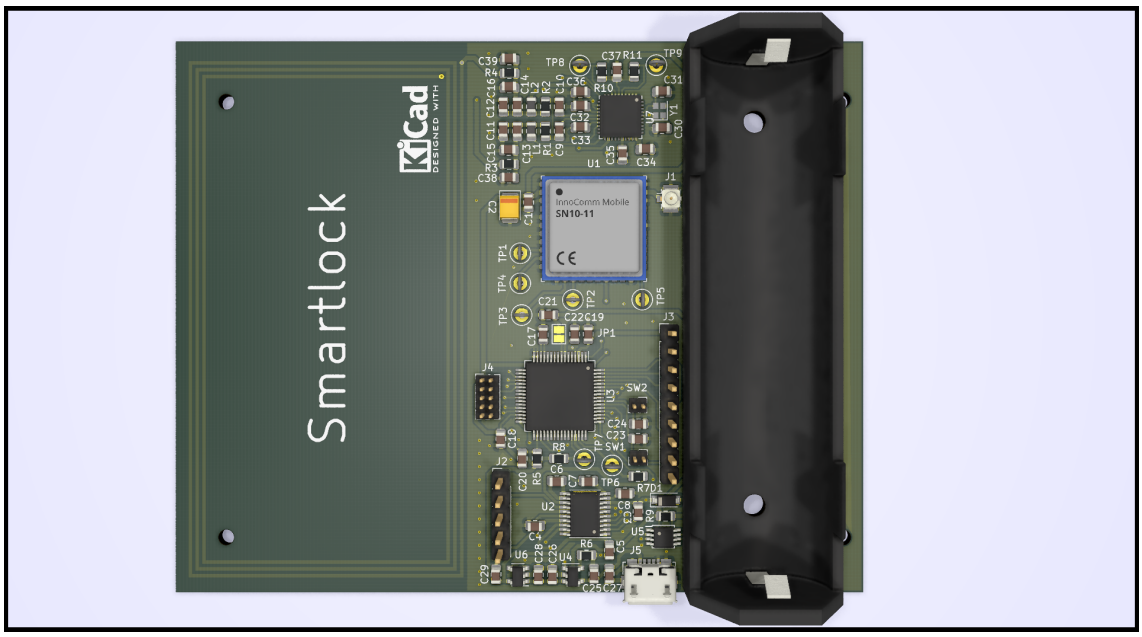
Obr. B.1: Osazovací plán DPS

Smartlock

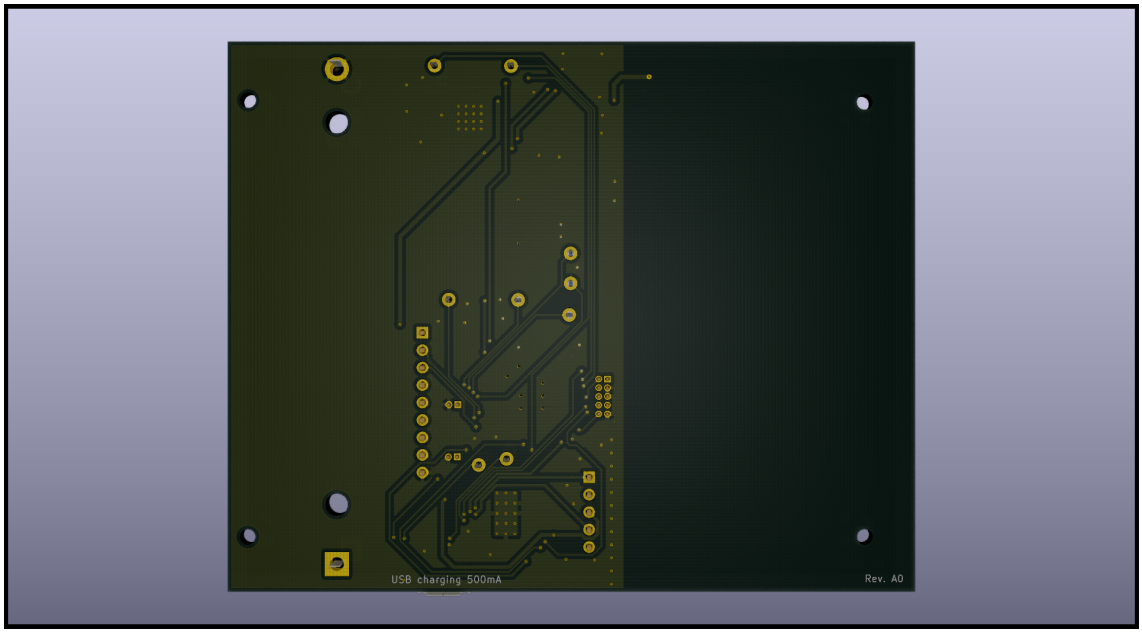

TP3
TP4
TP1
TP2
TP5
TP8
TP9
BT1
C30
Y1
C31
C29
C28
C26
C25
C27
C20
R5
C17
C21
C22
C19
C18
C23
C24
C1
C2
C3
C4
C5
C6
C7
C8
C9
C10
C11
C12
C13
C14
C15
C16
C32
C33
C34
C35
C36
C37
C38
C39
L1
R1
R2
R3
R4
R6
R7
R8
R9
U1
U2
U3
J1
J2
J3
J4
SW1
SW2

Rev. A0

C 3D vizualizace desky plošných spojů

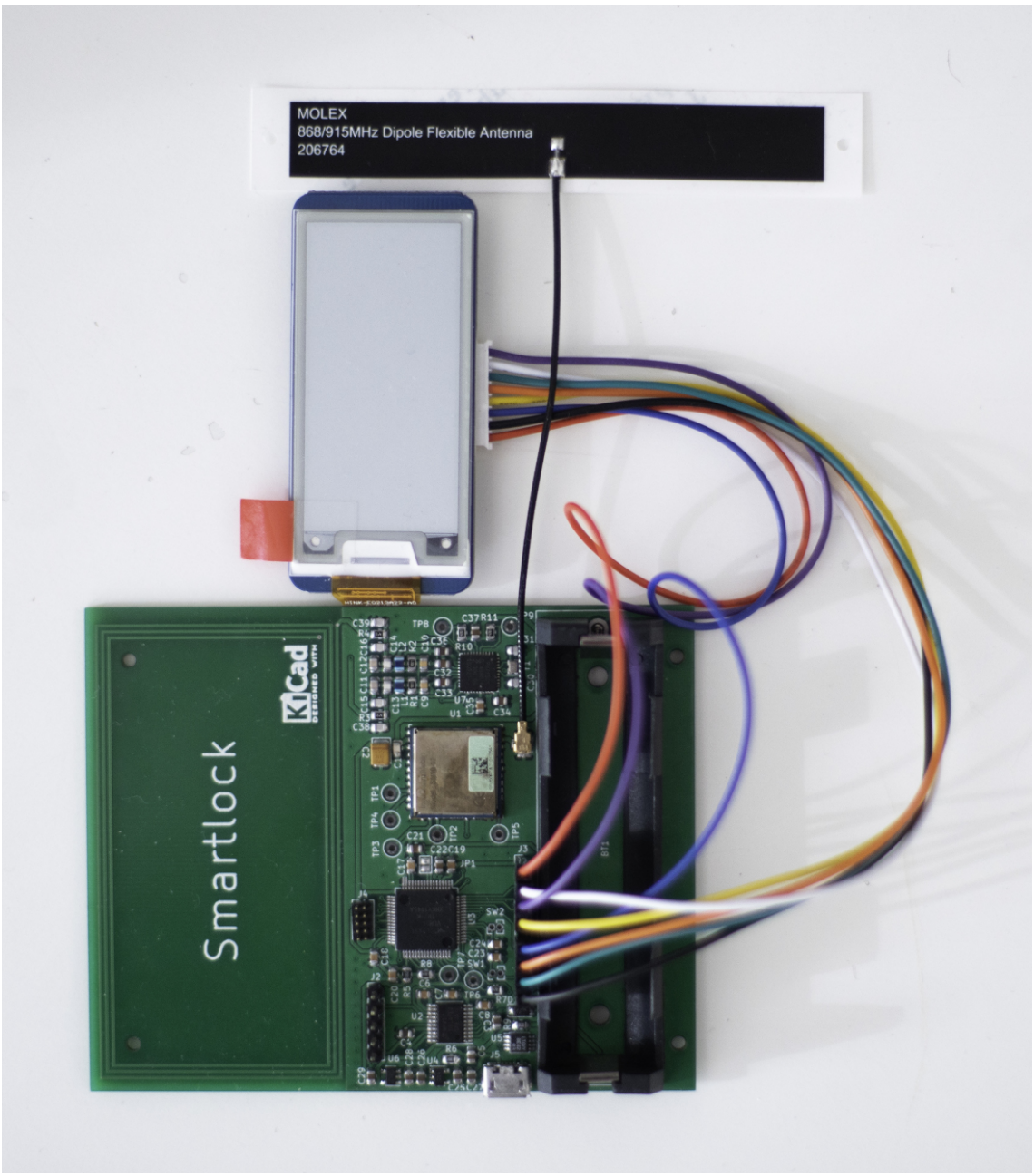


Obr. C.1: Pohled na DPS z vrchu



Obr. C.2: Pohled na DPS ze spodu

D Fotodokumentace



Obr. D.1: Fotografie výsledné DPS včetně displeje a Sigfox antény

Obr. D.2: Fotografie prototypu zámku na zmenšených dveřích, zadní strana

Obr. D.3: Fotografie prototypu zámku na zmenšených dveřích, přední strana

Obr. D.4: Demonstrace otevření dveří pomocí NFC tagu

Obr. D.5: Odesíláni zprávy do sítě Sigfox po odemčení zámku

E Seznam a cena materiálu

Cena materiálu byla získána pomocí softwaru KiCost z databází Octopart. Pro porovnání byly vybrány následující distributoři: Mouser, Farnell, Digi-Key. Texim Europe byl vybrán, protože je to jediný distributor čipu InnoComm SN10-11 pro Evropu.

V tabulce jsou zeleně zvýrazněné buňky, kde daný distributor nabízí nejlepší cenu. Oranžová barva značí momentální nedostupnost skladových zásob. Cena byla počítána pro výrobu tří kusů.

Prj: Smartlock
Co.: Marek Vitula
Prj date: 12/14/2019 8:41:50 PM
$ date: 2019-12-14 20:49:52

Global Part Info

Refs	Value	Footprint
AE2	Antenna Sigfox	Antenna:sigfox
BT1	Battery_Cell	Battery:BatteryHolder_MPD_BH-18650-PC2
C1	33p	Capacitor_SMD:C_0805_2012Metric
C11,C12	250p/16V	Capacitor_SMD:C_0805_2012Metric
C13,C14	30p/50V	Capacitor_SMD:C_0805_2012Metric
C15,C16	150p/50V	Capacitor_SMD:C_0805_2012Metric
C2	47u/10V	Capacitor_Tantalum_SMD:CP_EIA-3528-21_Kemet-B
C28,C32-C34,C37	1u	Capacitor_SMD:C_0805_2012Metric
C3,C4,C25-C27,C36	4.7u	Capacitor_SMD:C_0805_2012Metric
C30,C31	10pF	Capacitor_SMD:C_0805_2012Metric
C38,C39	5p/50V	Capacitor_SMD:C_0805_2012Metric
C5,C21,C22,C29	2.2u	Capacitor_SMD:C_0805_2012Metric
C9,C10	1n	Capacitor_SMD:C_0805_2012Metric
C6-C8,C17-C20,C23,C24,C35	100n	Capacitor_SMD:C_0805_2012Metric
D1	MMSZ5237BT1G	Diode_SMD:D_SOD-123
J1	Hirose U.FL	Connector_Coaxial:U.FL_Hirose_U.FL-R-SMT-1_Vertical
J2	Conn_01x05	Connector_PinHeader_2.54mm:PinHeader_1x05_P2.54mm_Vertical
J3	Conn_01x09	Connector_PinHeader_2.54mm:PinHeader_1x09_P2.54mm_Vertical
J4	Conn_ARM_JTAG_SWD_10	Connector_PinHeader_1.27mm:PinHeader_2x05_P1.27mm_Vertical
J5	USB_B_Micro	Connector_USB:USB_Micro-B_Molex_47346-0001
L1,L2	470n	Inductor_SMD:L_0805_2012Metric
R1,R2	1k	Resistor_SMD:R_0805_2012Metric
R3,R4	2.4R	Resistor_SMD:R_0805_2012Metric
R5	10k	Resistor_SMD:R_0805_2012Metric
R6	2k	Resistor_SMD:R_0805_2012Metric
R7,R8,R10,R11	4k7	Resistor_SMD:R_0805_2012Metric
R9	10m	Resistor_SMD:R_0805_2012Metric
SW1,SW2	SW_Push	Connector_PinHeader_1.27mm:PinHeader_1x02_P1.27mm_Vertical
U1	INNOCOMM-SN10-11	Antenna:InnoCommSN10-11
U2	MPC17531ATEJ	Package_SO:HTSSOP-20-1EP_4.4x6.5mm_P0.65mm_EP3.4x6.5mm_ThermalVias
U3	K32L2B21VLH0A	Package_QFP:LQFP-64_10x10mm_P0.5mm
U4	MCP73831-2-OT	Package_TO_SOT_SMD:SOT-23-5
U5	LTC2941CMS8E	Package_SO:MSOP-8-1EP_3x3mm_P0.65mm_EP1.68x1.88mm
U6	TPS78330	Package_TO_SOT_SMD:SOT-23-5
U7	PN7150	Package_DFN_QFN:QFN-40-1EP_6x6mm_P0.5mm_EP4.6x4.6mm
Y1	XRCGB27M120F3M10R0	Crystal:Crystal_SMD_2016-4Pin_2.0x1.6mm

Board Qty:	**3**						
Unit Cost:	**CZK1,047.28**						
Total Cost:	**CZK3,141.85**	**CZK2,376.06**	**CZK1,504.56**	**CZK2,790.10**	**CZK924.34**		
				Digi-Key	**Farnell**	**Mouser**	**Texim**
Manf#	**Qty**	**Unit$**	**Ext$**	**Ext$**	**Ext$**	**Ext$**	**Ext$**
206764-0100	3	CZK62.45	CZK187.36	CZK250.18	CZK187.36	CZK250.18	
1043	3	CZK60.44	CZK181.31	CZK181.31	CZK211.88	CZK181.31	
C0805C330K5HACAUTO	3	CZK0.52	CZK1.56	CZK1.56		CZK10.54	
08055A251JAT2A	6	CZK6.79	CZK40.76			CZK40.76	
08055A300GAT2A	6	CZK2.85	CZK17.08	CZK17.08		CZK66.06	
08055A151FAT2A	6	CZK7.96	CZK47.79	CZK49.19	CZK48.33	CZK47.79	
TPSB476M010T0250	3	CZK8.15	CZK24.46	CZK24.46		CZK87.14	
C0805C105K8RACTU	15	CZK1.08	CZK16.16	CZK62.55	CZK25.04	CZK16.16	
C0805C475K8PACTU	18	CZK1.92	CZK34.58	CZK75.05	CZK53.06	CZK34.58	
SQCFVA100JATME	6	CZK21.79	CZK130.71	CZK130.71		CZK130.71	
08055A5R0CAT2A	6	CZK3.98	CZK23.89	CZK23.89		CZK23.89	
C0805C225K8RACTU	12	CZK3.30	CZK39.64	CZK45.54	CZK66.54	CZK39.64	
C0805C102J5GAC7210	6	CZK3.05	CZK18.27			CZK18.27	
C0805C104K8RACTU	30	CZK3.51	CZK105.41	CZK105.41	CZK128.70	CZK105.41	
MMSZ5237BT1G	3	CZK4.69	CZK14.06	CZK14.06	CZK14.36	CZK14.06	
U.FL-R-SMT-1(10)	3	CZK21.13	CZK63.39	CZK92.06	CZK63.39	CZK83.63	
5-146274-5	3	CZK5.50	CZK16.50	CZK16.50	CZK40.97	CZK26.00	
22-30-3093	3	CZK4.47	CZK13.40	CZK13.79	CZK13.40	CZK30.92	
M50-3500542	3	CZK25.80	CZK77.40	CZK83.63	CZK77.40	CZK83.63	
47346-0001	3	CZK21.22	CZK63.65	CZK73.79	CZK63.65	CZK66.76	
LQW21HNR47J00L	6	CZK11.71	CZK70.28	CZK70.28		CZK70.28	
RT0805FRE071KL	6	CZK2.29	CZK13.76	CZK14.06	CZK13.76	CZK16.87	
ESR10EZPF2R40	6	CZK0.39	CZK2.32	CZK2.32		CZK22.49	
RT0805FRE0710KL	3	CZK2.34	CZK7.03	CZK7.03	CZK7.49	CZK8.43	
RT0805FRE072KL	3	CZK2.34	CZK7.03	CZK7.03		CZK8.43	
RT0805FRE134K7L	12	CZK1.50	CZK17.99			CZK17.99	
CFN0805-FX-R010ELF	3	CZK12.42	CZK37.25	CZK43.57		CZK37.25	
M50-3530242	6	CZK1.52	CZK9.11	CZK16.87	CZK9.11	CZK15.46	
SN10-11-INNO	10	CZK92.43	CZK924.34				CZK924.34
MPC17531ATEJ	3	CZK58.56	CZK175.69	CZK175.69	CZK182.11	CZK175.69	
K32L2B21VLH0A	3	CZK69.43	CZK208.30	CZK208.30		CZK282.51	
MCP73831T-3ACI/OT	3	CZK13.12	CZK39.35	CZK39.35	CZK40.71	CZK39.35	
LTC2941CMS8E#PBF	3	CZK73.25	CZK219.76	CZK229.10	CZK219.76	CZK229.10	
C0805C475K8PACTU	3	CZK2.95	CZK8.84	CZK18.27	CZK8.84	CZK11.95	
PN7150B0HN/C11004Y	3	CZK85.81	CZK257.44	CZK257.44		CZK470.85	
XRCGB27M120F3M10R0	3	CZK8.67	CZK26.00	CZK26.00	CZK28.72	CZK26.00	